

## CHAPTER 18

# Networking Practices

### In this chapter, you will learn:

- How to connect a computer or small network to the Internet using a broadband, satellite, or dial-up connection
- How to configure a SOHO router and set up a wireless network
- About tools and utilities used to troubleshoot problems with network and Internet connections
- How to troubleshoot connectivity problems with networks and client applications

**I**n the last chapter, you learned about hardware used to build a network and how to connect a computer to an existing network. This chapter takes the next logical step in learning about networking by discussing connections to the Internet using Windows and how to set up a Small Office Home Office (SOHO) network. You will then learn about several tools and utilities that you will need when supporting a small wired or wireless network. Finally, you will learn how to troubleshoot problems when network and Internet connections fail.

Security is always a huge concern when dealing with networks. In this chapter, you will learn how to use a software and hardware firewall to protect a network. In the next chapter, we take security to a higher level and discuss all the many tools and techniques you can use to protect a single computer or a SOHO network.



#### **A+ Exam Tip**

All the content in this chapter applies to networking objectives on the A+ 220-702 Practical Application exam.

## CONNECTING TO THE INTERNET

A+  
220-702  
3.2

In this part of the chapter, you'll learn how to connect a single PC to the Internet and then how to use Windows Firewall to protect that connection. Later in the chapter, you'll learn how to use a router to create a more sophisticated and secure Internet connection that can support multiple computers all accessing the Internet.

You need to know how to connect to the Internet when using cable modem, DSL, satellite, dial-up, and ISDN connections. All these types of connections are covered in the following sections.

**A+ Exam Tip**

The A+ 220-702 Practical Application exam expects you to know how to connect to the Internet when using a DSL, cable modem, satellite, ISDN, or dial-up connection.

Generally, when setting up a cable modem or DSL connection to the Internet, the installation goes like this:

1. Connect the PC to the cable modem or DSL box. Connect the cable modem to the TV jack or the DSL box to the phone jack. Plug in the power and turn on the broadband device.
2. Configure the TCP/IP settings for the connection to the ISP.
3. Test the connection by using a browser to surf the Web.

Now let's look at the specific details of making a cable modem connection or DSL connection to the Internet.

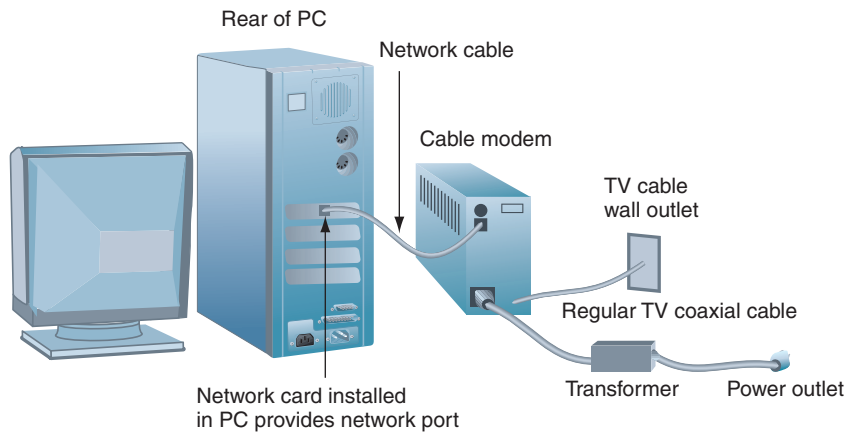
### CONNECT TO THE INTERNET USING CABLE MODEM

To set up a cable modem installation to the Internet, you'll need the following:

- ▲ Internet service provided by your cable modem company.
- ▲ A computer with an available network or USB port.
- ▲ A cable modem and a network or USB cable to connect to the PC.
- ▲ The TCP/IP settings to use to configure TCP/IP provided by the cable modem company. For most installations, you can assume dynamic IP addressing is used. If static IP addressing is used, you'll need to know the IP address, the IP address of one or two DNS servers, the subnet mask, and the IP address of the default gateway (the IP address of a server at the ISP).

The setup for a cable modem connection using a network cable is shown in Figure 18-1. Follow these instructions to connect a computer to the Internet using a cable modem connection, an Ethernet cable to connect the PC to the modem, and dynamic IP addressing:

1. Select the TV wall jack that will be used to connect your cable modem. You want to use the jack that connects directly to the point where the TV cable comes into your home, with no splitters between this jack and the entrance point. Otherwise, in-line splitters can degrade the signal quality and make your connection erratic. The cable company can test each jack and tell you which jack is best to use for the cable modem—one good reason to have a technician come and hook you up for the first time. Later, if your cable modem connection is constantly going down, you might consider that you've chosen the wrong jack for the connection.



**Figure 18-1** Cable modem connecting to a PC through a network card installed in the PC  
 Courtesy: Course Technology/Cengage Learning

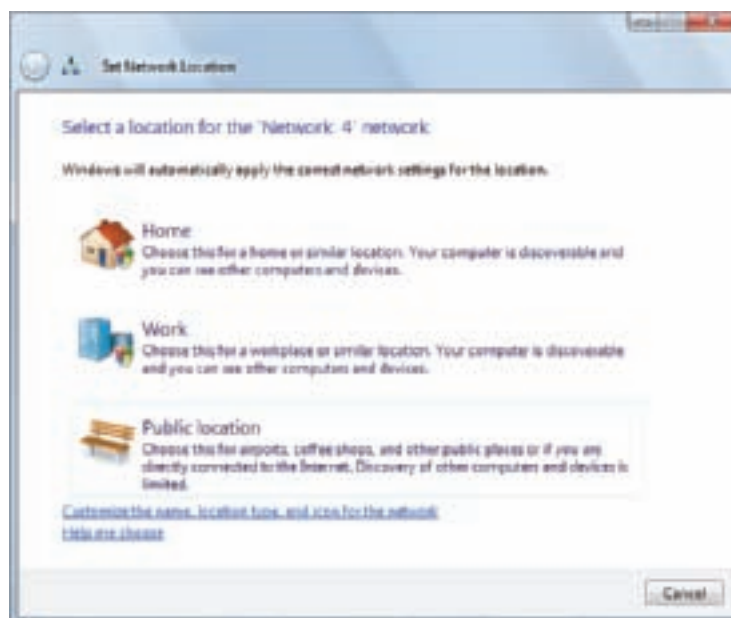
2. Using coaxial cable, connect the cable modem to the TV wall jack. Plug in the power cord to the cable modem.
3. When using a network port on your PC, connect one end of the network cable to the network port on the PC, and the other end to the network port on the cable modem.



#### Tip

A network cable is sometimes called an Ethernet cable or a patch cable. A network port can also be called an Ethernet port. You need to be familiar with all these terms, and they are all used in this chapter.

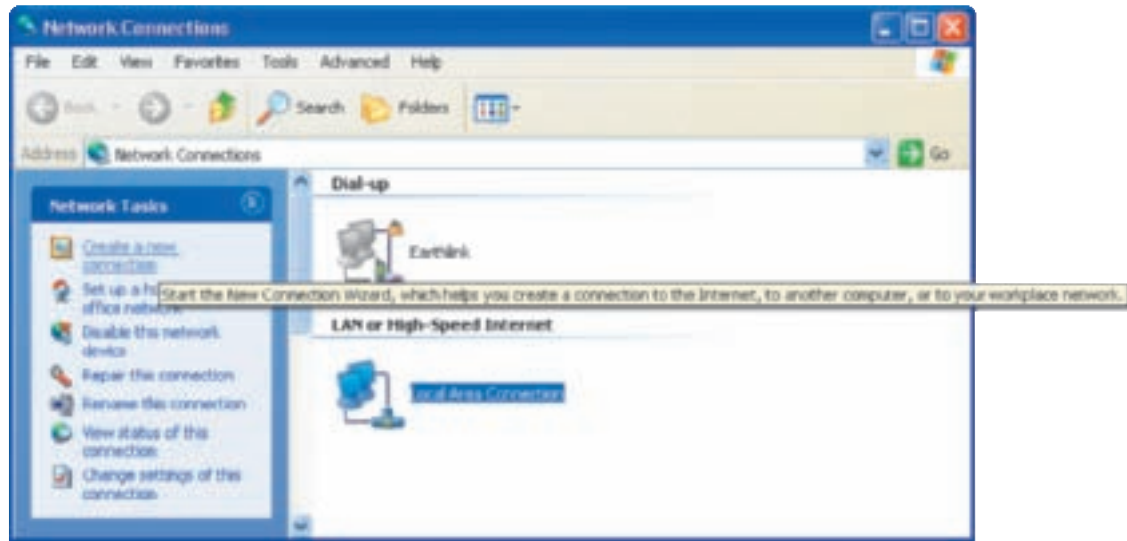
4. Vista automatically creates a new always-up network connection and displays the Set Network Location window shown in Figure 18-2. Select the location, most likely **Home**.



**Figure 18-2** Vista asks for the location of the new connection so that it can configure the firewall  
 Courtesy: Course Technology/Cengage Learning

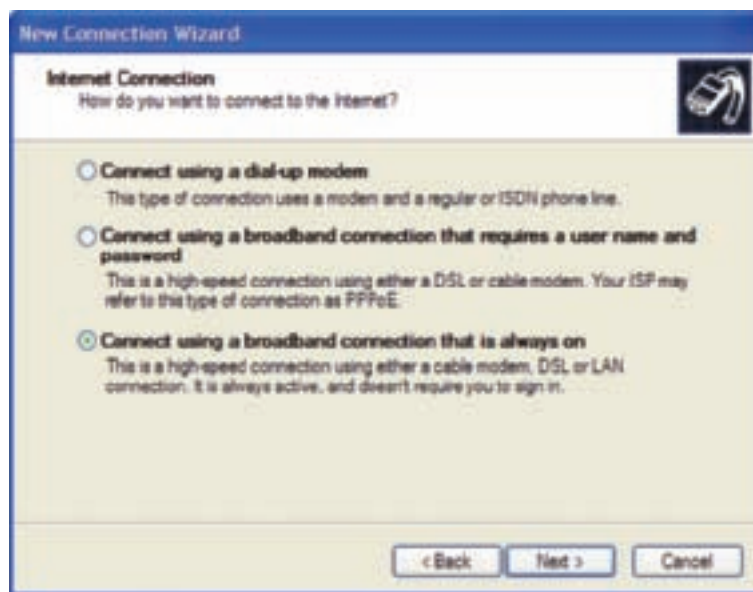
A+  
220-702  
3.2

5. For Windows XP, right-click **My Network Places** and select **Properties** from the shortcut menu. The Network Connections window opens. See Figure 18-3. Click **Create a new connection**.



**Figure 18-3** Using Windows XP, launch the New Connection Wizard  
Courtesy: Course Technology/Cengage Learning

6. The New Connection Wizard opens. Click **Next** to skip the welcome screen. On the next screen, select **Connect to the Internet** and click **Next**.
7. On the next screen, select **Set up my connection manually** and click **Next**. On the following screen (see Figure 18-4), select **Connect using a broadband connection that is always on** and then click **Next**. The wizard creates the connection. Click **Finish** to close the wizard.



**Figure 18-4** Choose the type of Internet connection  
Courtesy: Course Technology/Cengage Learning

**Notes** When setting up a cable modem, you might want to connect your TV to the same jack that the cable modem is using. In this situation, connect a splitter to the jack and then connect the cable modem and TV cables to the splitter. If the connection gives problems, try removing the splitter.

Follow these directions if you are using a USB cable to connect your cable modem to your computer:

1. When using a USB port on your PC, first read the directions that came with your cable modem to find out if you should install the software before or after you connect the cable modem. For most installations, you begin by connecting the cable modem.
2. Connect the USB cable to your PC and to the cable modem. Plug in and turn on the cable modem and Windows will automatically detect it as a new USB device. When the Found New Hardware Wizard launches (see Figure 18-5), click **Locate and install driver software**, respond to the UAC box, and insert the USB driver CD that came with your cable modem. The wizard searches for and installs these drivers.



**Figure 18-5** When using a USB cable to connect to the cable modem, the Found New Hardware Wizard will install the cable modem drivers  
Courtesy: Course Technology/Cengage Learning

3. You can now pick up with Step 4 above to configure the Vista or XP connection.

After the connection is configured in Windows, you are ready to activate your service and test the connection. Do the following:

1. The cable company must know the MAC address of the cable modem you have installed. If you have received the cable modem from your cable company, the company already has the MAC address listed as belonging to you and you can skip this step. If you purchased the cable modem from another source, look for the MAC address somewhere on the back or bottom of the cable modem. See Figure 18-6. Contact the cable company and tell them the new MAC address.

A+  
220-702  
3.2



**Figure 18-6** Look for the MAC address of the cable modem printed on the modem  
Courtesy: Course Technology/Cengage Learning

2. Test the Internet connection using your Web browser. If you are not connected, try the following:
  - a. For Vista, open the Network and Sharing Center window and select **Diagnose and repair** under Tasks. This will walk you through a few basic steps to try to resolve the issue. For XP, in the Network Connections window, select the network connection and then click **Repair this connection**.
  - b. If this doesn't work, turn off the PC and the cable modem. Wait a full five minutes until all connections have timed out at the cable company. Turn on the cable modem and wait for the lights on the front of the modem to settle in. Then turn on the PC. After the PC boots up, again check for connectivity.
  - c. Try another cable TV jack in your home.
3. If this doesn't work, call the cable company's help desk. The technician there can release and restore the connection at that end, which might restore service. If this doesn't work, there might be a problem with the cable company's equipment, which the company will need to repair.

## CONNECT TO THE INTERNET USING DSL

DSL service and an older technology, ISDN, are provided by the local telephone company. (An up-and-coming, second-generation DSL, called DSL over Fiber in the Loop [DFITL], uses dedicated fiber-optic cable to bring DSL to your neighborhood.) A DSL installation works pretty much the same way as a cable modem installation.

Here are the steps that are different:

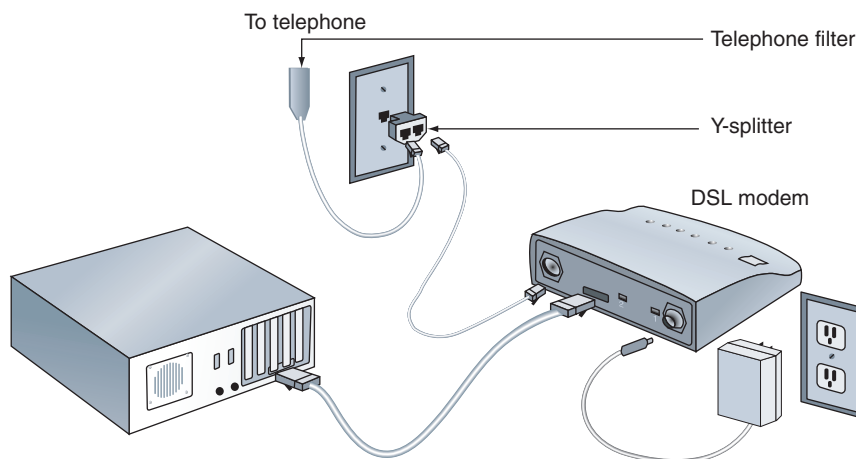
1. Read the directions that came with the DSL modem and follow them. If your DSL modem came with a setup CD, you can run that setup to step you through the installation, including installing the drivers for a modem that uses a USB connection. You might be instructed to run a setup CD on your PC before you connect the modem, or you might need to install the modem first.

2. To prevent static on the line, install a telephone filter on every phone jack in your house that is being used by a telephone, fax machine, or dial-up modem. See Figure 18-7.



**Figure 18-7** A DSL filter is required to eliminate static on regular telephones  
Courtesy: Course Technology/Cengage Learning

3. Connect the DSL modem as shown in Figure 18-8. If necessary, you can use a Y-splitter on the wall jack (as shown in Figure 18-8) so that a telephone can use the same jack. Be sure to add a filter between the splitter and the telephone; the filter also appears in the diagram. On the other hand, you can use a filter such as that shown in Figure 18-7 that can plug directly into the wall jack and serve both a telephone and the DSL modem. Plug the DSL modem into the DSL port on a filter or directly into a wall jack. (Don't connect the DSL modem to a telephone port on the filter; this setup would prevent DSL from working.) Plug in the power to the DSL modem. Connect a network cable or USB cable between the DSL modem and the PC.



**Figure 18-8** Sample setup for DSL  
Courtesy: Course Technology/Cengage Learning



A+  
220-702  
3.2

4. Follow the steps given earlier to use Vista or XP to configure the DSL connection, which works the same way as with cable modem.
5. Open your browser and surf the Web to test the connection.
6. If you did not receive the DSL modem from the telephone company, you might need to call the DSL help desk and give them the MAC address of the modem and have them reset the connection on their end.

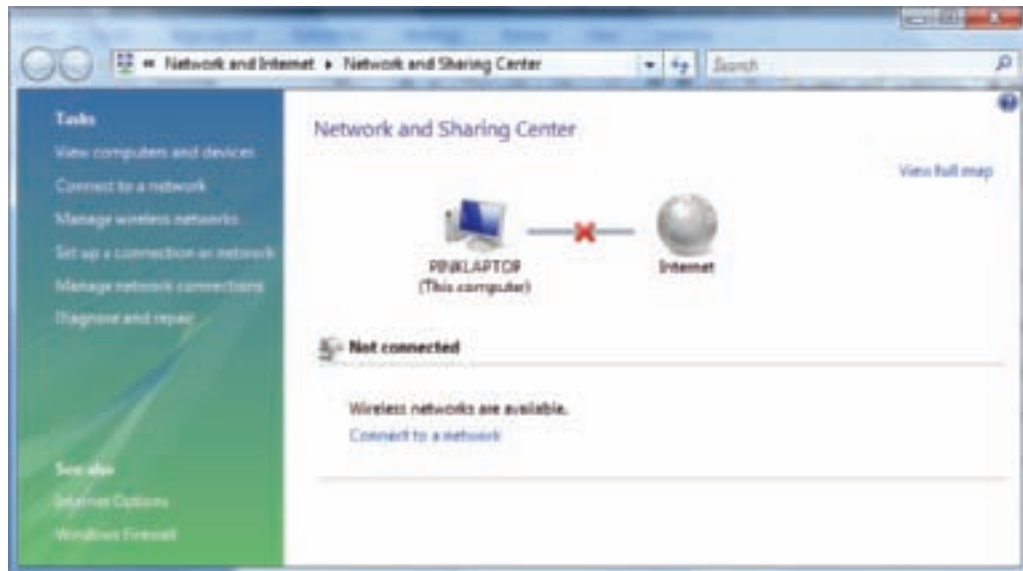
If your DSL connection requires a user name and password or static IP addressing, see the next section on how to configure these connections.

### **CONNECT TO THE INTERNET USING AN ON-DEMAND BROADBAND CONNECTION OR STATIC IP ADDRESSING**

Most broadband connections today are always up and use dynamic IP addressing, which are the assumptions that Vista and XP make when they create and configure a new network connection. But some business services for cable modem or DSL use static IP addressing, and a less expensive DSL service might use an on-demand connection.

Follow these steps to create an on-demand broadband connection to the Internet:

1. Follow directions given in this chapter to connect the cable modem or DSL modem to the PC and to connect the modem to the wall jack. Vista will automatically create a new connection configured with dynamic IP addressing and an always-up connection.
2. Click **Start**, right-click **Network**, and select **Properties** from the shortcut menu. The Network and Sharing Center window opens. See Figure 18-9.

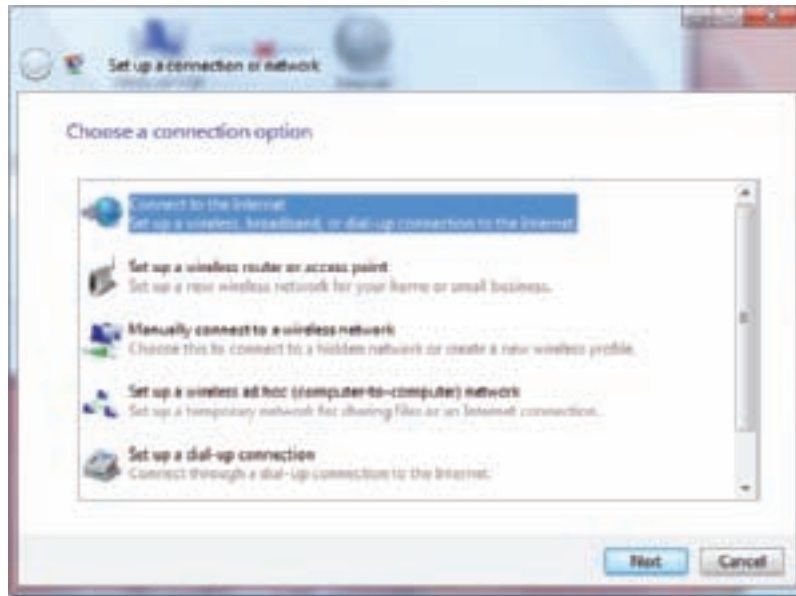


**Figure 18-9** Use the Network and Sharing Center to create and manage network connections  
Courtesy: Course Technology/Cengage Learning

3. Click **Set up a connection or network**. On the next screen (see Figure 18-10), select **Connect to the Internet** and click **Next**.



A+  
220-702  
3.2

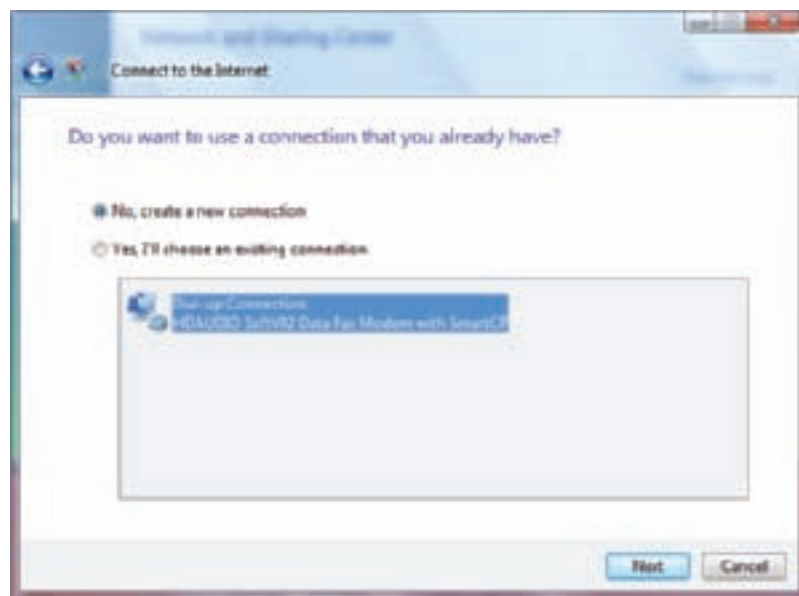


**Figure 18-10** Select the type of network you want to set up  
Courtesy: Course Technology/Cengage Learning

**Notes**

An on-demand broadband connection that is not always up requires that a user name and password be authenticated at the ISP each time you make the connection. The logon is managed by a protocol called PPPoE (Point-to-Point-Protocol over Ethernet), which is why the connection is sometimes called a PPPoE connection.

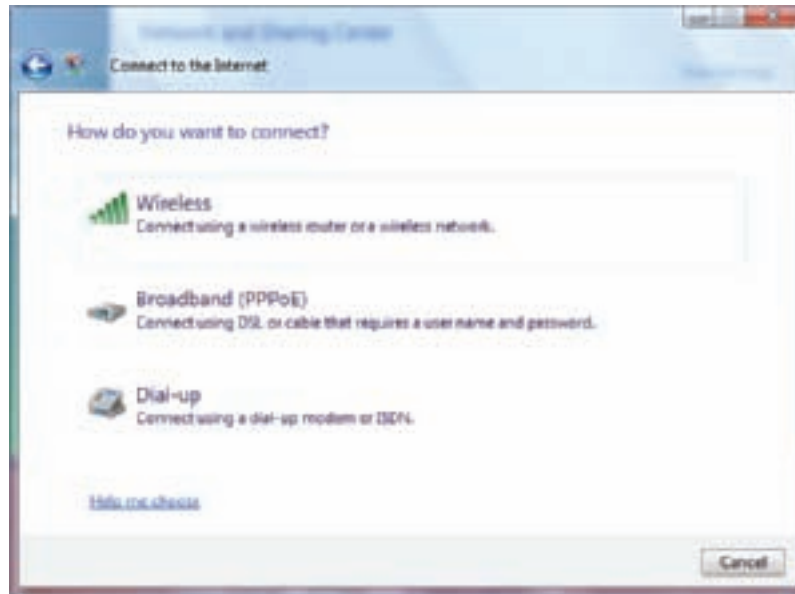
4. If the computer has other network connections that are not currently active, the screen in Figure 18-11 appears. Select **No, create a new connection** and click **Next**.



**Figure 18-11** Choose the option to create a new network connection  
Courtesy: Course Technology/Cengage Learning

A+  
220-702  
3.2

5. On the next screen shown in Figure 18-12, click **Broadband (PPPoE)**.



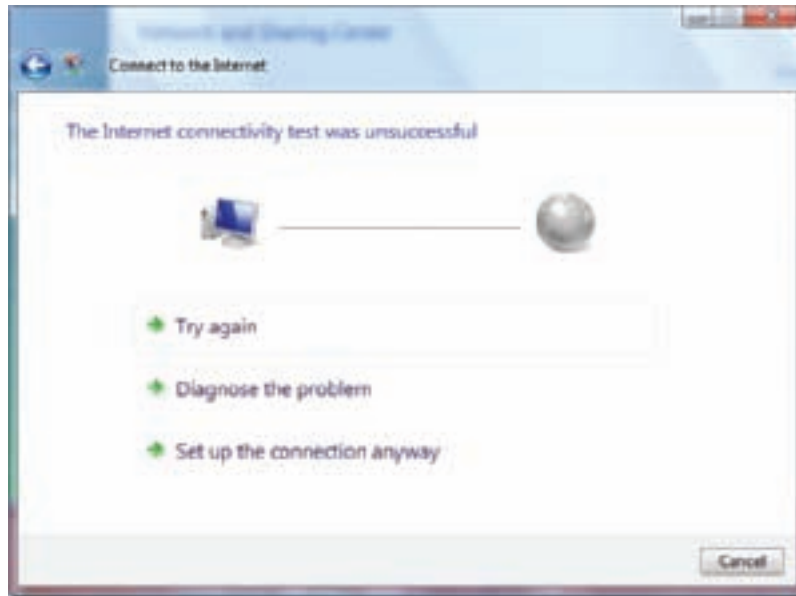
**Figure 18-12** Choose to create a broadband connection  
Courtesy: Course Technology/Cengage Learning

6. On the next screen (see Figure 18-13), fill in the information for the User name and Password given to you by your ISP. The Connection name can be any name you like. At the bottom of the screen there is also a check box that will allow other users on this computer to use the connection. Click **Connect**.



**Figure 18-13** Enter the information given to you by your ISP  
Courtesy: Course Technology/Cengage Learning

7. Vista assumes the connection will use dynamic IP addressing and attempts to make the connection. If you are using static IP addressing, the connection will fail and you will see the screen in Figure 18-14. For that situation, click **Set up the connection anyway**. On the next screen, click **Close**.



**Figure 18-14** The connection failed  
Courtesy: Course Technology/Cengage Learning

8. For Windows XP, you can configure an on-demand connection when first configuring the network connection using the New Connection Wizard. The window on the wizard that you use is shown earlier in Figure 18-4. Click **Connect using a broadband connection that requires a user name and password**. Follow the wizard through to complete the on-demand setup.



**Notes** If your broadband subscription is not always up and requires you to enter your username and password each time you connect, using a router with auto-connecting ability can be a great help. It can automatically pass the username and password to your broadband provider without your involvement. The router can also be set to auto-refresh a connection before it expires.

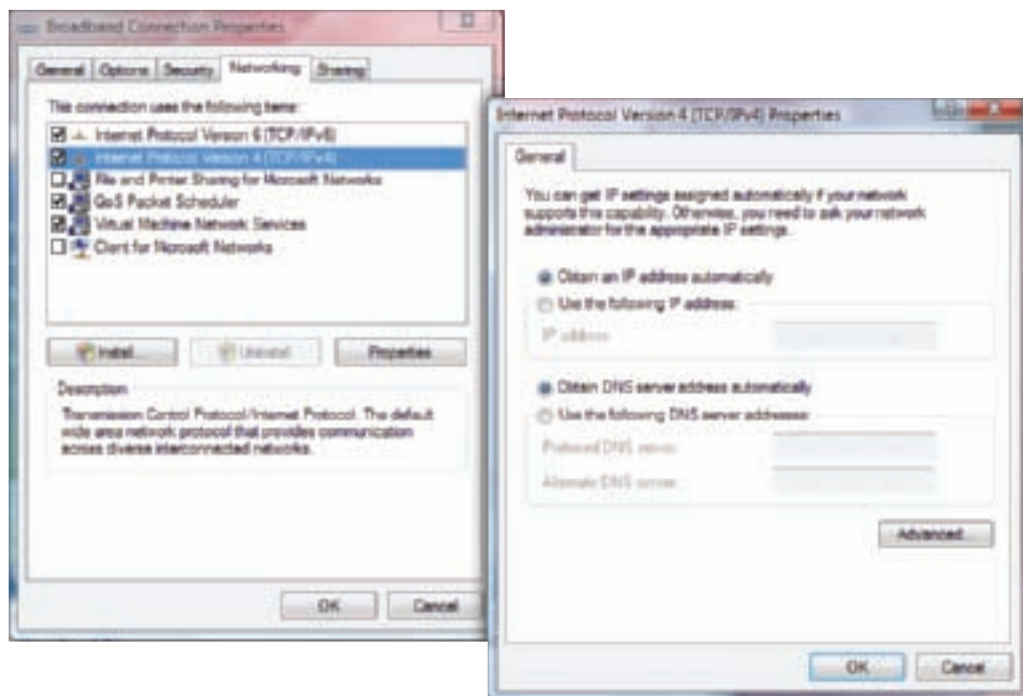
Follow these steps to configure a network connection for static IP addressing:

1. In the Vista Network and Sharing Center window, click **Manage network connections**. The Network Connections window appears, showing each network the computer has set up (see Figure 18-15). The broadband connection icon will have whatever name you gave it; the default name is Broadband Connection, as shown in the figure. Right-click **Broadband Connection**, select **Properties** from the shortcut menu, and respond to the UAC box. The Broadband Connection Properties box appears.
2. Select the **Networking** tab, which is shown in the left side of Figure 18-16. On this tab, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. The properties box appears, as shown on the right side of Figure 18-16.
3. For static IP addressing, select **Use the following IP address** and enter the IP address, subnet mask, and default gateway given to you by your ISP. Then enter the IP addresses given to you by your ISP for the first two DNS servers. If your ISP gave you IP addresses for a third or fourth DNS server, click **Advanced** and enter those IP addresses on the DNS tab in the Advanced TCP/IP Settings box and click **OK**.
4. Click **OK** twice to close the two dialog boxes. Then close the Network Connections window.

A+  
220-702  
3.2



**Figure 18-15** Use the Network Connections window to manage these connections  
Courtesy: Course Technology/Cengage Learning



**Figure 18-16** Use the Connection Properties box to configure IP addressing  
Courtesy: Course Technology/Cengage Learning

5. To configure a Windows XP network connection for static IP addressing, right-click the **Local Area Connection** icon in the Network Connections window, and then select **Properties** from the shortcut menu. (Local Area Connection is the default name for this icon; it might have been given a different name.) The properties box opens. Select **Internet Protocol (TCP/IP)** and click **Properties**. Configure the TCP/IP properties the same as with Windows Vista.

## CONNECT TO THE INTERNET USING SATELLITE

The Federal Communications Commission (FCC) requires that a trained technician install a satellite Internet service. The technician that does the installation will generally follow these steps:

1. The technician installs the satellite dish. For North America, the dish faces south with an unobstructed view of the southern sky.
2. Double coaxial cables are installed from the dish to the room in your building where the satellite modem will sit. The modem should sit near your computer or router.

3. Coaxial cables are plugged into two ports on the modem, most likely labeled Sat In and Sat Out. An Ethernet cable is connected to the RJ-45 port on the modem and the RJ-45 port on your PC.
4. The connection is configured in Windows. A satellite service is an always-up service that most likely uses dynamic IP addressing.

## CONNECT TO THE INTERNET USING A DIAL-UP CONNECTION

You never know when you might be called on to support an older dial-up connection. Here are the bare-bones steps you need to set up and support this type connection:

1. Install an internal or external dial-up modem. How to install a modem card is covered in Chapter 9. Make sure Device Manager recognizes the card without errors.
2. Plug the phone line into the modem port on your computer and into the wall jack.
3. For Vista, open the Network and Sharing Center window and click **Set up a connection or network**.
4. On the next window, select **Set up a dial-up connection** and click **Next**.
5. On the next window (see Figure 18-17), enter the phone number to your ISP, your ISP username and password, and the name you decide to give the dial-up connection, such as the name and city of your ISP. Then click **Connect**.
6. For Windows XP, click **Create a new connection** in the Network Connections window. Follow the steps of the wizard, which are similar to those of Vista.



**Figure 18-17** Configure a dial-up connection  
Courtesy: Course Technology/Cengage Learning

To use the connection, go to the Vista Network and Sharing Center and click **Connect to a network**. Select the dial-up connection, and click **Connect**. The Connect dialog box appears (see Figure 18-18). Click **Dial**. You will hear the modem dial up the ISP and make the connection. For XP, double-click the connection icon in the Network Connections window, and then click **Dial**.

A+  
220-702  
3.2



**Figure 18-18** Make a dial-up connection to your ISP  
Courtesy: Course Technology/Cengage Learning

To view or change the configuration for the dial-up connection, do the following:

1. In the Vista Network and Sharing Center, click **Manage network connections**, and then right-click **Dial-up Connection** (or other name assigned the connection) and select **Properties** from the shortcut menu. For XP, right-click the connection icon in the Network Connections window and select **Properties** from the shortcut menu. The connection Properties box opens, as shown in Figure 18-19 for Vista. The XP box is similar.



**Figure 18-19** Configure an Internet connection using the Properties window of the connection icon  
Courtesy: Course Technology/Cengage Learning



2. Use the tabs on this window to configure TCP/IP (Networking tab), control the way Windows attempts to dial the ISP when the first try fails (Options tab), and change other dialing features.

If the dial-up connection won't work, here are some things you can try:

- ▲ Is the phone line working? Plug in a regular phone and check for a dial tone. Is the phone cord securely connected to the computer and the wall jack?
- ▲ Does the modem work? Check Device Manager for reported errors about the modem. Does the modem work when making a call to another phone number (not your ISP)?
- ▲ Check the Dial-up Connection Properties box for errors. Is the phone number correct? Does the number need to include a 9 to get an outside line? Has a 1 been added in front of the number by mistake? If you need to add a 9, you can put a comma in the field like this "9,4045661200", which causes a slight pause after the 9 is dialed.
- ▲ Try dialing the number manually from a phone. Do you hear beeps on the other end?
- ▲ Try another phone number.
- ▲ When you try to connect, do you hear the number being dialed? If so, the problem is most likely with the phone number, the phone line, or the username and password.
- ▲ Is TCP/IP configured correctly? Most likely you need to set it to obtain an IP address automatically.
- ▲ Reboot your PC and try again.
- ▲ If the computer has two RJ-11 ports, try the other port.
- ▲ Try removing and reinstalling the dial-up connection.



**Notes** If you want to disable call waiting while you're connected to the Internet, enter \*70 in front of the phone number.

## CONNECT TO THE INTERNET USING ISDN

ISDN is an older, outdated technology and it's unlikely you'll ever be called on to set up an ISDN connection. But, just in case, here are a few essential tips that will make your work easier:

- ▲ The phone line that is handling the ISDN connection can support one or two ISDN connections or an ISDN connection and a regular telephone call.
- ▲ The ISDN equipment consists of an ISDN modem. The modem might also be able to serve double duty as a router for a small LAN.
- ▲ Logically, the ISDN modem contains two pieces of equipment. An NT1 (Network Terminator 1) device interfaces between the phone company and the home or business telephone network. A TA (terminal adapter) device interfaces with the local network. In most cases, both devices are contained in the modem box that uses an RJ-11 jack to connect to the telephone line and an RJ-45 jack to connect to the network.
- ▲ Charges for the ISDN line might be based on per-minute use. If that's the case, make sure your e-mail software or browser is not set to make the connection automatically when you don't want to incur a charge.
- ▲ When you first set up ISDN, connect the modem box and then configure the ISDN connection in the same way you would configure a dial-up connection using a regular phone line.



## IMPLEMENT WINDOWS FIREWALL AND VISTA NETWORK SECURITY

The Internet is a nasty and dangerous place infested with hackers, viruses, worms, and thieves. Knowing how to protect a single PC or a LAN is an essential skill of a PC support technician. The three most important things you can do to protect a single computer or network are to:

- ▲ Keep Windows updates current so that security patches are installed as soon as they are available.
- ▲ Use a software and/or hardware firewall.
- ▲ Run antivirus software and keep it current.

In earlier chapters, you learned how to keep Windows updates current. In the next chapter, you'll learn all about using antivirus software. In this section, you'll learn to use a software firewall and a hardware firewall. Software firewalls are appropriate when you're protecting a single personal computer that is connected directly to the Internet or is part of a local network. A hardware firewall, such as a multipurpose router, is used to protect all computers on the network from malicious activity coming from the Internet. In this part of the chapter, you'll learn to use a software firewall. Later in the chapter, you'll learn how to set up a hardware firewall.

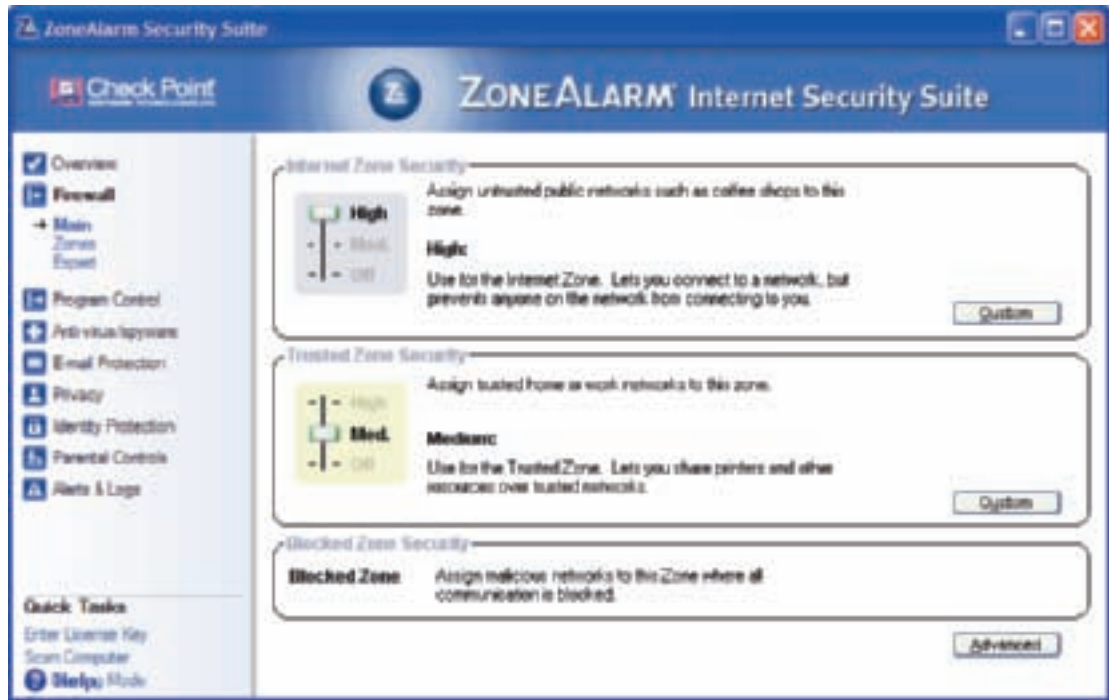
A hardware or software firewall can function in several ways:

- ▲ Firewalls can filter data packets, examining the destination IP address or source IP address or the type of protocol used (for example, TCP or UDP).
- ▲ Firewalls can filter ports so that outside client applications or programs cannot communicate with inside services listening at these ports. Certain ports can be opened, for example, when your network has a Web server and you want Internet users to be able to access it.
- ▲ Firewalls can block certain activity that is initiated from inside the network—such as preventing users behind the firewall from using applications like FTP over the Internet. When evaluating firewall software, look for its ability to control traffic coming from both outside and inside the network.
- ▲ Some firewalls can filter information such as inappropriate Web content for children or employees, and can limit the use of the Internet to certain days or times of the day.

Some examples of firewall software are ZoneAlarm (see Figure 18-20) by Check Point Software ([www.zonealarm.com](http://www.zonealarm.com)), Firewall Software Blade by Check Point Software ([www.checkpoint.com](http://www.checkpoint.com)), and Windows Firewall. In addition, Norton 360 by Symantec ([www.symantec.com](http://www.symantec.com)) and McAfee VirusScan Plus by McAfee ([www.mcafee.com](http://www.mcafee.com)) include antivirus software as well as a software firewall.

Windows Vista automatically configures Windows Firewall based on the type of network it believes you are connected to. Vista can assign you a public profile, a private profile, or a domain profile. A **public profile** offers the highest level of protection when you are connected to a public network. A **private profile** offers moderate protection when you are connected to a private network, and the least protection is used for a **domain profile**, when your PC is on a domain and security is managed by the domain's operating system, such as Windows Server 2008. When a PC first connects to a new network that is not part of a domain, Vista asks you if the network is a public or private network (refer back to Figure 18-2). It saves this response and applies it each time you reconnect to this network. Windows XP automatically sets the firewall for a moderate level of protection.

A+  
220-702  
3.2



**Figure 18-20** ZoneAlarm allows you to determine the amount of security the firewall provides  
Courtesy: Course Technology/Cengage Learning

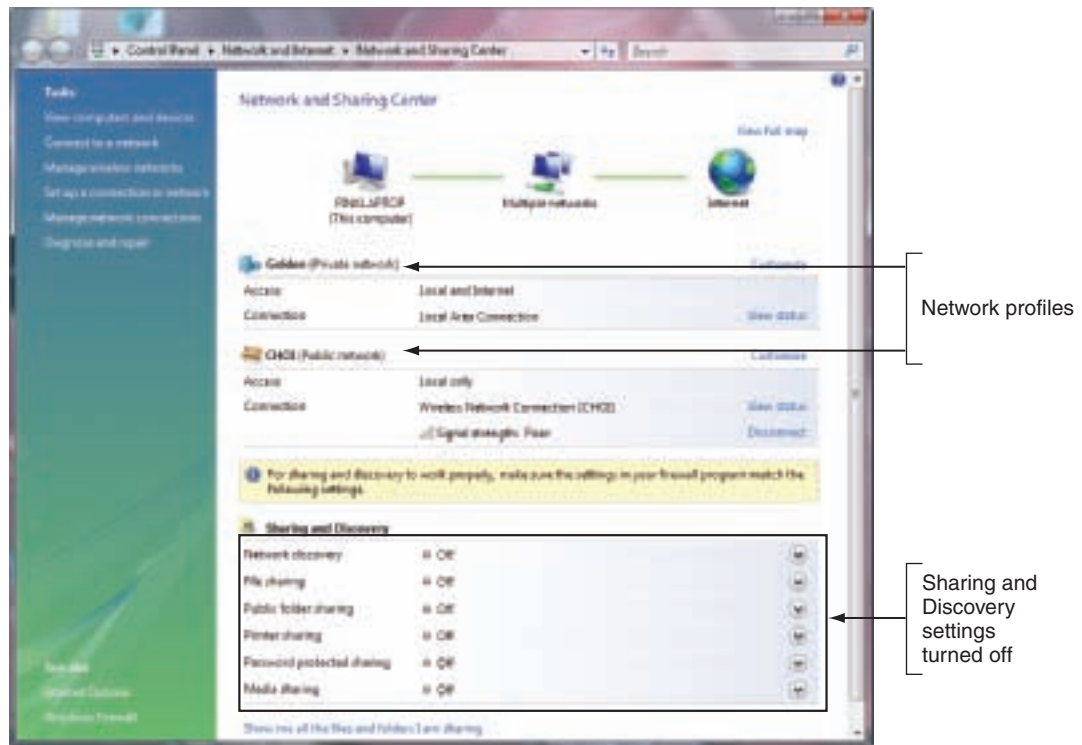
For Windows Vista, to see how firewall protection is set for a public or private network, use the Network and Sharing Center window by following these steps:

1. Click **Start**, right-click **Network**, and select **Properties** from the shortcut menu. The Network and Sharing Center window opens.
2. For the window showing in Figure 18-21, the PC is connected to a wired and wireless network. The wired network is set to Private and the wireless network is set to Public. Because the PC is connected to a public network, the Sharing and Discovery settings at the bottom of the window are turned off. To change the security setting for the Public network, click **Customize**.
3. The Set Network Location box appears (see Figure 18-22). To allow for less security and more communication on the network, click **Private** and then click **Next**.
4. Sharing and Discovery settings are now less secure, allowing the PC to be seen on the network (Network discovery), files on the PC to be shared with others on the network (File sharing), and printers installed on this PC to be shared (Printer sharing). These are the standard settings for a private network. To change a setting under the Sharing and Discovery group, click the down arrow to the right of the item and turn the item on or off (see Figure 18-23). In Chapter 19, you will learn to use Windows Explorer to share files and folders on the network.

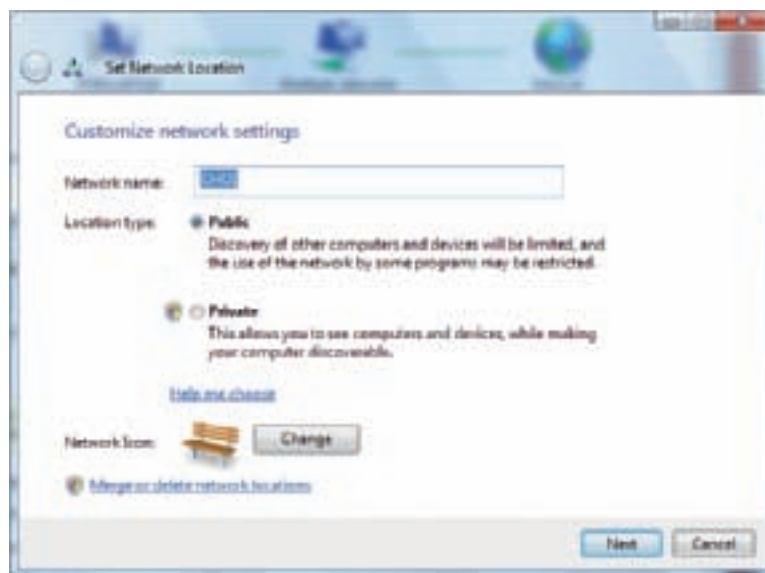
To see how Windows Firewall is configured for Vista, follow these steps:

1. For Vista, in the left pane of the Network and Sharing Center window, click **Windows Firewall**. The Windows Firewall dialog box opens (see Figure 18-24). No matter what type of network you are connected to, Windows Firewall should always be turned on unless you are using a third-party software firewall instead of Windows Firewall.

A+  
220-702  
3.2

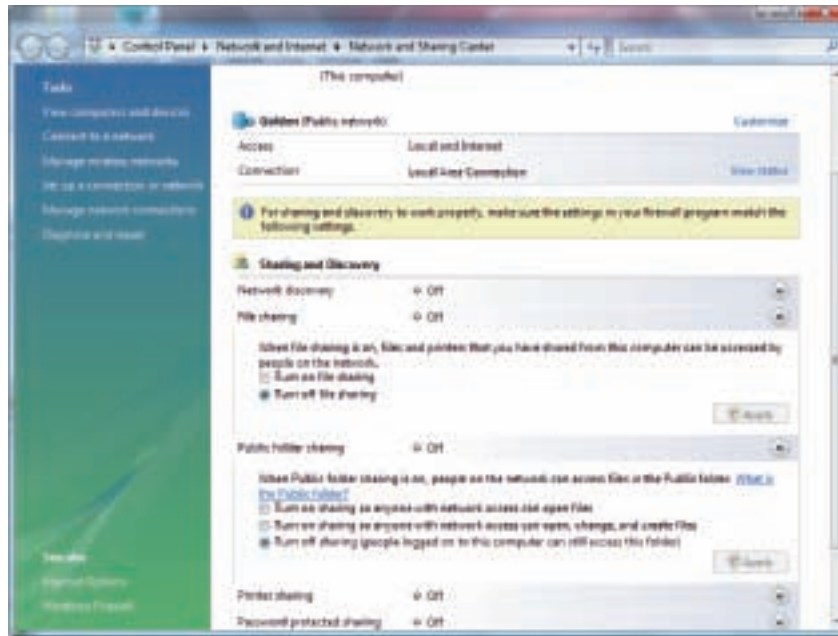


**Figure 18-21** Security is high when connected to a public network  
Courtesy: Course Technology/Cengage Learning

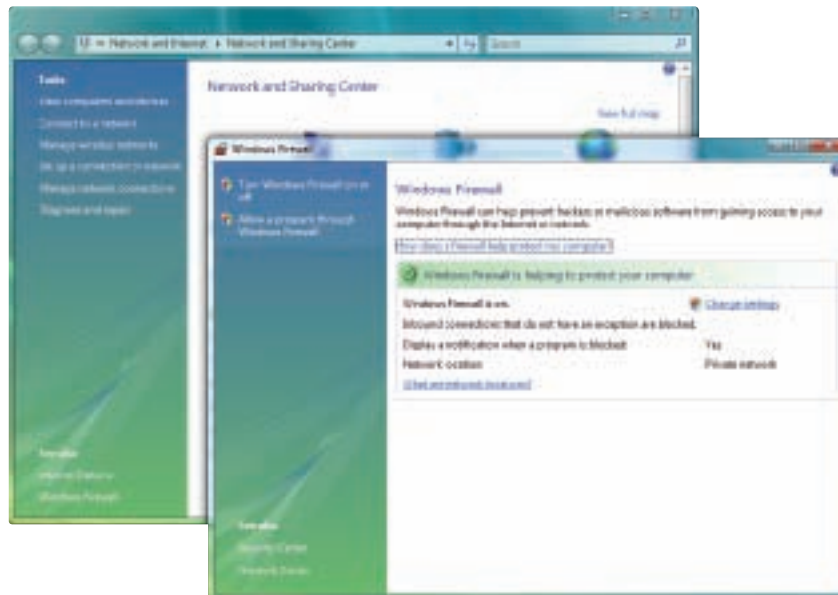


**Figure 18-22** Change the security settings for a network  
Courtesy: Course Technology/Cengage Learning

A+  
220-702  
3.2



**Figure 18-23** Change the setting of an item under the Sharing and Discovery group  
 Courtesy: Course Technology/Cengage Learning



**Figure 18-24** Windows Firewall is turned on  
 Courtesy: Course Technology/Cengage Learning

A+  
220-702  
3.2

2. To see the details of how Windows Firewall is working, click **Change settings** and respond to the UAC box. The Windows Firewall Settings box opens (see Figure 18-25).



**Figure 18-25** Windows Firewall is on but not working at its highest security level  
Courtesy: Course Technology/Cengage Learning

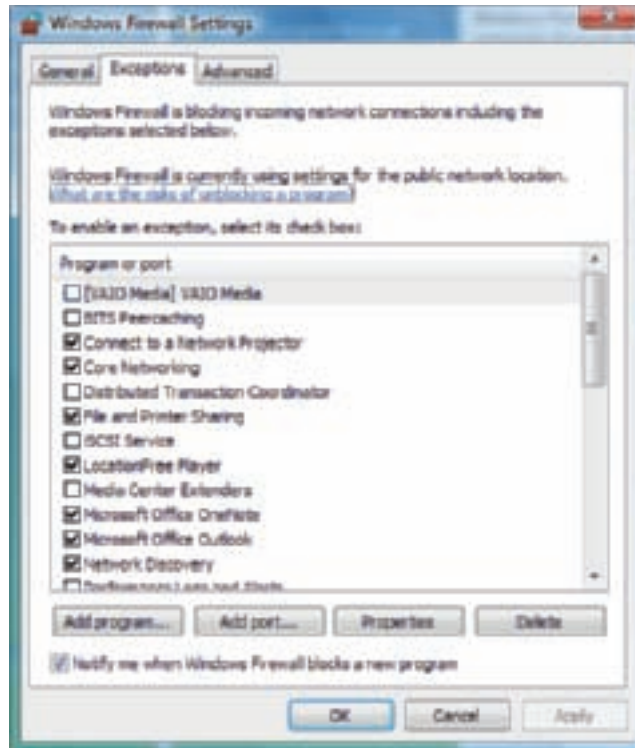
3. Notice the check box for *Block all incoming connections*, which controls communication initiated from another computer. For a private network, Vista does not check this box. When connected to a public network, the box is checked. To see what incoming connections are allowed, click the **Exceptions** tab (see Figure 18-26).
4. Notice in Figure 18-26 that File and Printer Sharing is checked. This means that another computer can initiate communication with this computer to access a shared file or printer. You can change individual settings on this Exceptions tab by checking or unchecking items. Recall from Chapter 17 that a computer uses a port number to control incoming activity from client applications or programs on the network. This Exceptions box controls these ports. Each item in the list is associated with one or more ports, which are opened or closed based on the settings on this tab.

After you have Windows Firewall configured the way you want it, click **Apply** and click **OK** to close the Windows Firewall Settings window.

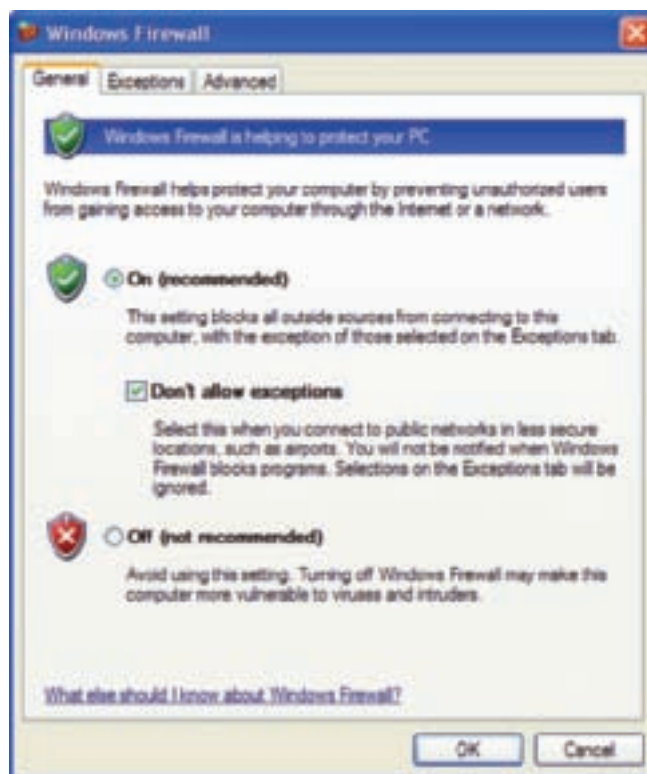
To view and change the Windows Firewall settings for Windows XP, use the Network Connections window. In the left pane, click **Change Windows Firewall settings**. The Windows Firewall window opens, as shown in Figure 18-27. Verify that **On (recommended)** is selected.



A+  
220-702  
3.2



**Figure 18-26** Exceptions allowed for incoming connections  
Courtesy: Course Technology/Cengage Learning



**Figure 18-27** Windows Firewall for Windows XP is set for maximum protection  
Courtesy: Course Technology/Cengage Learning

A+  
220-702  
3.2

If you don't want to allow any communication to be initiated from remote computers, check **Don't allow exceptions**. This is the preferred setting when you're traveling or using public networks or Internet connections. If you are on a local network and need to allow others on the network to access your computer, uncheck **Don't allow exceptions**. Then click the **Exceptions** tab to select the exceptions to allow. For example, if you want to share files and folders on your local network, use the Exceptions tab to allow File and Printer Sharing activity.

Later in the chapter, you'll learn how to use the Exceptions tab of Windows Firewall to allow certain client applications such as Remote Desktop access to your computer.

## SETTING UP A SOHO NETWORK

A PC support technician is likely to be called on to set up a small office or home office network. To set up this network, you need to know how to physically connect computers to a network and how to install and configure a multipurpose router to stand between the network and the Internet. And, finally, you need to know how to set up and secure a wireless access point. All these skills are covered in this part of the chapter.

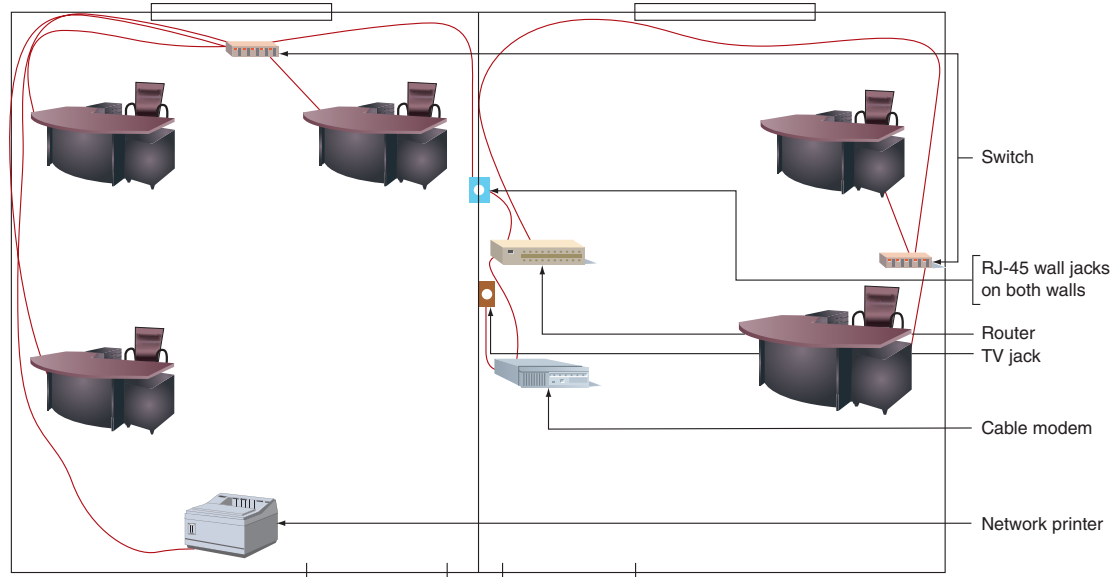
### PHYSICALLY CONFIGURE A SMALL NETWORK

To set up a small network, you'll need computers, switches, network cables, a router, and whatever device (for example, a DSL or cable modem) that provides Internet access. Recall from the last chapter that a switch is used to connect two or more computers by way of Ethernet patch cables (also called network cables). Some network cables might be wired inside walls of your building with wall jacks that use RJ-45 ports. If network cables are lying on the floor, be sure to install them against the wall so they won't be a trip hazard. Take care that cables don't exceed the recommended length. Recall from Chapter 17 that 10BaseT, 100BaseT, and 1000BaseT Ethernet networks (also called Ethernet, Fast Ethernet, and Gigabit Ethernet) can use UTP or STP cables no longer than 100 meters (328 feet). For Fast Ethernet or Gigabit Ethernet, always use twisted-pair cables rated at CAT5e or higher. To connect multiple computers, use switches rated at the same speed as your router and network adapters. For best results, buy Gigabit switches and network adapters, a Gigabit router, and CAT6 cables. However, if some devices run at slower speeds, most likely a switch or router can still support the higher speeds for other devices on the network.

If your router is also your wireless access point, take care in planning where to place it. Place the wireless access point near the center of the area where you want your wireless network. The router also needs to have access to your cable modem, DSL modem, or whatever device that provides Internet access. That device needs access to the cable TV or phone jack where it receives service. Figure 18-28 shows a possible inexpensive wiring job where two switches and a router are used to wire two rooms for five workstations and a network printer. The only inside-wall wiring that is required is two back-to-back RJ-45 wall jacks on either side of the wall between the two rooms. The plan allows for all five desktop computers and a network



A+  
220-702  
3.2



**Figure 18-28** Plan the physical configuration of a small network  
Courtesy: Course Technology/Cengage Learning

printer to be wired with cabling neatly attached to the baseboards of the office without being a trip hazard.

## INSTALL AND CONFIGURE A ROUTER FOR A SMALL NETWORK

To install a router that comes with a setup CD, run the setup program on one of your computers on the network (doesn't matter which one). Follow the instructions on the setup screen to disconnect the cable modem or DSL modem from your host computer and connect it to the router. Next, connect the computers on your network to your router. A computer can connect directly to a network port on the router, or you can connect a switch or hub to one port on the router. The switch or hub can then provide multiple ports for computers to connect. Plug in the router and power it on.

You'll be required to sign in to the utility using a default password. The first thing you want to do is reset this password so that others cannot change your router setup.



### Caution

Changing the router password is especially important if the router is a wireless router. Unless you have disabled or secured the wireless access point, anyone outside your building can use your wireless network. If they guess the default password to the router, they can change the password to hijack your router. Also, your wireless network can be used for criminal activity. When you first install a router, before you do anything else, change your router password and disable the wireless network until you have time to set up and test the wireless security. And, to give even more security, change the default name to another name if the router utility allows that option.

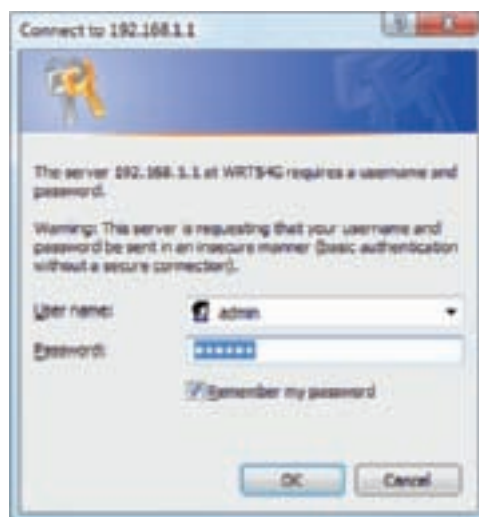
A+  
220-702  
3.2

The setup program will then step you through the process of configuring the router. After you've configured the router, you might have to turn the cable modem or DSL modem off and back on so that it correctly syncs up with the router. If you don't get immediate connectivity to the Internet on all PCs, try refreshing the IP address or rebooting each PC.

Now let's look at how a Linksys router, such as the one shown in Figure 18-29, is configured. The methods are typical of what you might see for several brands and models of small office or home office routers. Firmware on the router (which can be flashed for updates) contains a configuration program that you access using a Web browser from anywhere on the network. In your browser address box, enter the IP address of the router (for our router, it's 192.168.1.1) and press **Enter**. A logon box appears (see Figure 18-30). Use the account name and password given in the router documentation to sign in.



**Figure 18-29** This router by Linksys allows computers on a LAN to share a broadband Internet connection and is an access point for computers with wireless adapters  
Courtesy: Course Technology/Cengage Learning



**Figure 18-30** Log in to the router configuration utility  
Courtesy: Course Technology/Cengage Learning

A+  
220-702  
3.2

The main Setup window appears, as shown in Figure 18-31. For most situations, the default settings on this and other screens should work to provide network access without any changes.

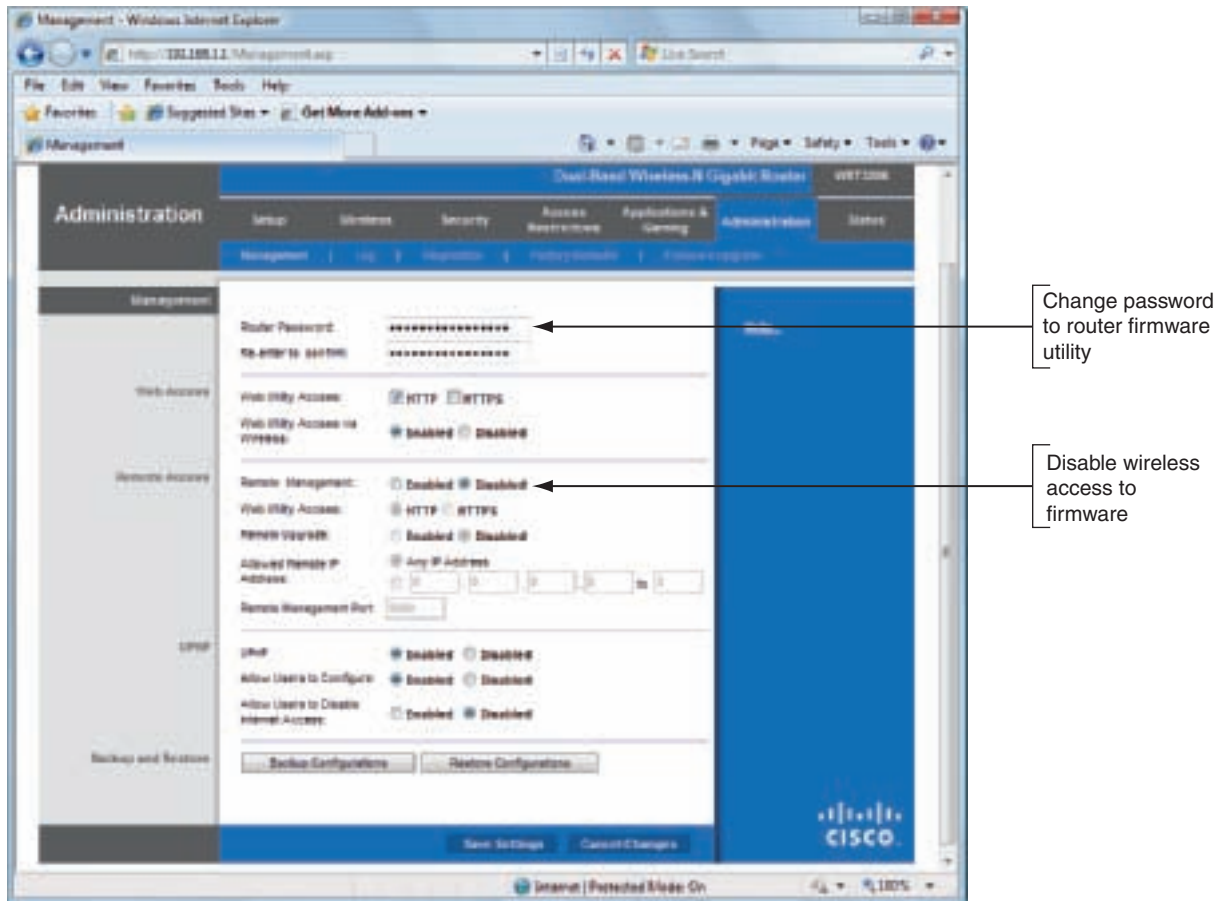


**Figure 18-31** Basic Setup screen used to configure the router  
Courtesy: Course Technology/Cengage Learning

A+  
220-702  
3.2

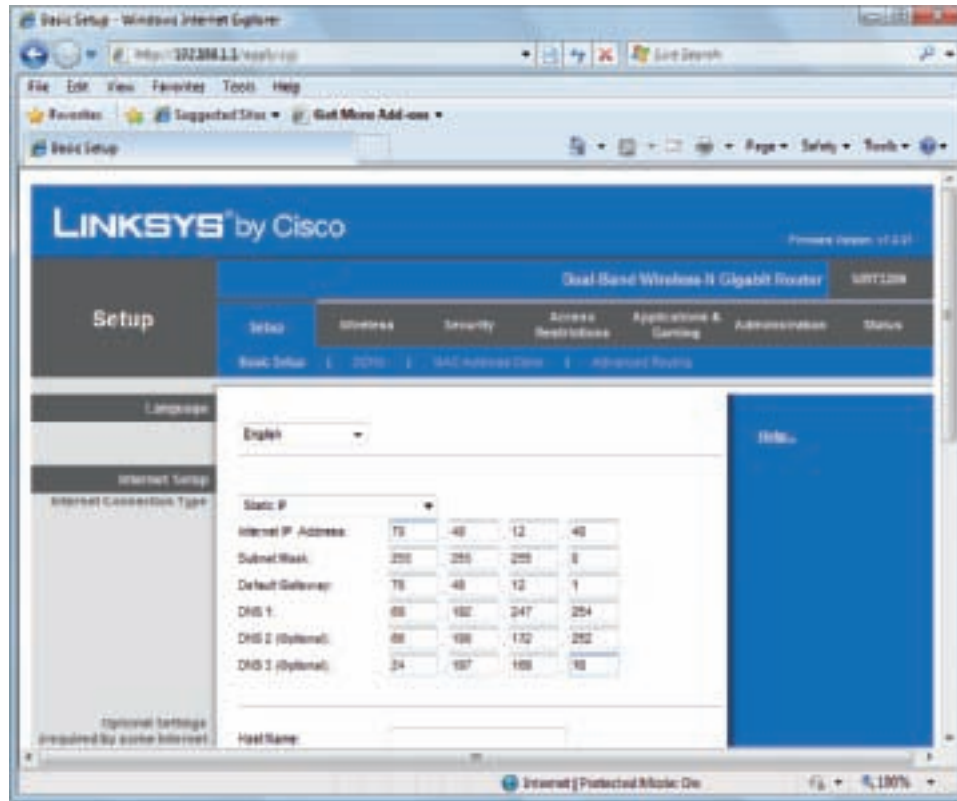
Following are some changes that you might need to make to the router's configuration. The first one should always be done:

- It's extremely important to protect access to your network and prevent others from hijacking your router. Do that by changing the password to the router firmware. If the firmware offers the option, disable the ability to configure the router from over the wireless network (see Figure 18-32).



**Figure 18-32** Prevent others from hijacking your router  
Courtesy: Course Technology/Cengage Learning

- In the Internet Setup area, dynamic IP addressing is called Automatic Configuration — DHCP. If a host name and domain name have been given to you by your ISP, enter them here. Most likely, you'll leave them blank.
- If your ISP has assigned you a static IP address, click the drop-down box near the top of the Internet Settings area and change this setting to Static IP (see Figure 18-33). You can then enter the IP address assigned to you by your ISP as well as the subnet mask and IP addresses of the default gateway and DNS servers.
- You can configure the DHCP server under Network Setup in Figure 18-31. Notice in the figure that the router is configured to serve up to 50 leased IP addresses beginning with IP address 192.168.1.100. You can also disable the DHCP server if you want to use static IP addressing on your network or you already have another DHCP server on the network.
- One or more computers on your network might require a static IP address. For example, in the last chapter, you learned how to set up and use a Telnet server. Recall that you could access the server from another computer by using the host name of the



**Figure 18-33** Configure the router for static IP addressing  
Courtesy: Course Technology/Cengage Learning

server. The host name was associated to the server's IP address by making an entry in the Hosts file on the local computer. To make this entry always work, the Telnet server needs a static IP address. To set the router to serve up this same IP address to the Telnet server each time it connects to the network, click **DHCP Reservation** in Figure 18-31. You will then be able to enter a reserved IP address and the MAC address of the computer (Telnet server in our example) that is to receive this reserved IP address.

- ▲ If you have problems with the router or decide to keep firmware updates current, these updates can be downloaded and installed. First download the upgrade file from the Web site of the router manufacturer. Be sure to download the correct file for your router model and verify the firmware version is higher than the version already installed. If the router offers the option, back up the current firmware before you start the update. Next, to update the router firmware using the downloaded file, click the **Administration** tab and then click **Firmware Upgrade**. On the Firmware Upgrade window (see Figure 18-34), click **Browse** and point to the downloaded file. Then click **Upgrade** to begin the update. Don't disturb the router until the update has completed.

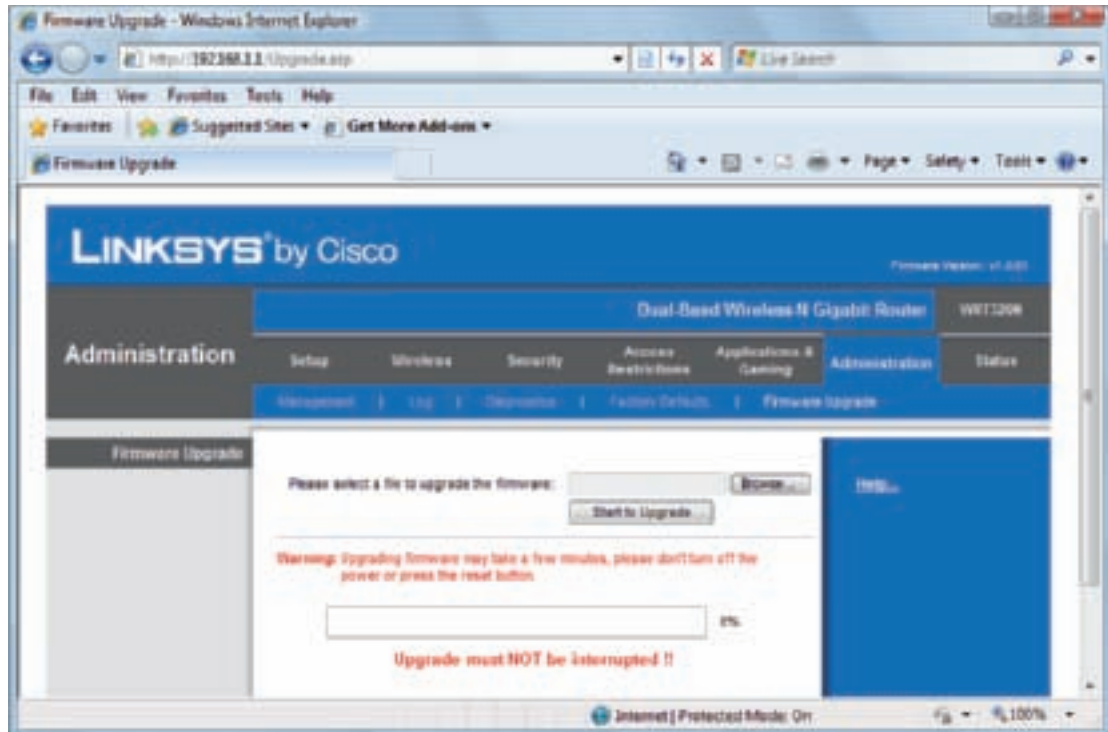
## CONFIGURE THE HARDWARE FIREWALL

To configure the hardware firewall router feature, you need to do the following:

- ▲ In the window shown in Figure 18-31, click the **Security** link. The window shown in Figure 18-35 appears. The most important setting on this window is to enable SPI Firewall Protection. SPI (stateful packet inspection) examines each data packet and rejects those unsolicited by the local network. Enabling this feature prevents your network from being detected or accessed (without an invitation) by others on the Internet.



A+  
220-702  
3.2



**Figure 18-34** Upgrade the router firmware  
Courtesy: Course Technology/Cengage Learning



**Figure 18-35** Configure the router's firewall to prevent others on the Internet from seeing or accessing your network  
Courtesy: Course Technology/Cengage Learning

- You can set policies to determine how and when users on your network can access the Internet. To do that, click **Access Restrictions**. The window shown in Figure 18-36 appears, allowing you to set policies about the day and time of Internet access, the services on the Internet that can be used, and the URLs and keywords that are not allowed.

The screenshot shows the 'Access Restrictions' configuration page for a 'Wireless-N Gigabit Router'. The page has a sidebar with navigation links: 'Applied PCs', 'Access Restriction', 'Schedule', 'Website Blocking by URL Address', 'Website Blocking by Keyword', and 'Blocked Applications'. The main content area is titled 'Internet Access Policy' and contains the following fields and controls:

- Access Policy:** A dropdown menu showing '1 (1)' with buttons for 'Delete This Entry' and 'Summary'.
- Enter Policy Name:** A text input field.
- Status:** Radio buttons for 'Enabled' and 'Disabled'.
- URL List:** A button labeled 'Edit URL' with a note: '(This Policy applies only to PCs on the List.)'
- Deny/Allow:** Radio buttons for 'Deny' and 'Allow'. The 'Allow' option is selected, and a note says 'Internet access during selected days and hours.'
- Schedule:**
  - Days:** Checkboxes for 'Everyday', 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', and 'Sat'. 'Everyday' is checked.
  - Time:** A time range selector with '24 Hours' selected, and fields for '12 AM', '00', '12 AM', and '00'.
- URL Blocking:** Fields for 'URL 1', 'URL 2', 'URL 3', and 'URL 4'.
- Keyword Blocking:** Fields for 'Keyword 1', 'Keyword 2', 'Keyword 3', and 'Keyword 4'.
- Blocked Applications:** A table with columns 'Applications' and 'Blocked List'. The 'Applications' column lists protocols and their port ranges: 'TCP (25-25)', 'RDP (33-33)', 'HTTP (80-80)', 'HTTPS (443-443)', 'FTP (21-21)', 'RPC (110-110)', and 'MAP (143-143)'. The 'Blocked List' column is empty. Below the table are fields for 'Application Name', 'Port Range', and 'Protocol'.

At the bottom of the page are buttons for 'Add', 'Modify', and 'Delete'.

**Figure 18-36** Configure the router's firewall to limit Internet access from within the network  
 Courtesy: Course Technology/Cengage Learning

## PORT FORWARDING AND PORT TRIGGERING

Too much security is not always a good thing. There are legitimate times you want to be able to access computers on your network from somewhere on the Internet or allow others to do so, such as when you're hosting an Internet game or when you're traveling and want to use Remote Desktop to access your home computer. In this section, we'll look at how to drop your shields low enough so that the good guys can get in but the bad guys can't. However, know that when you drop your shields the least bit, you're compromising the security of your network, so be sure to use these methods sparingly.

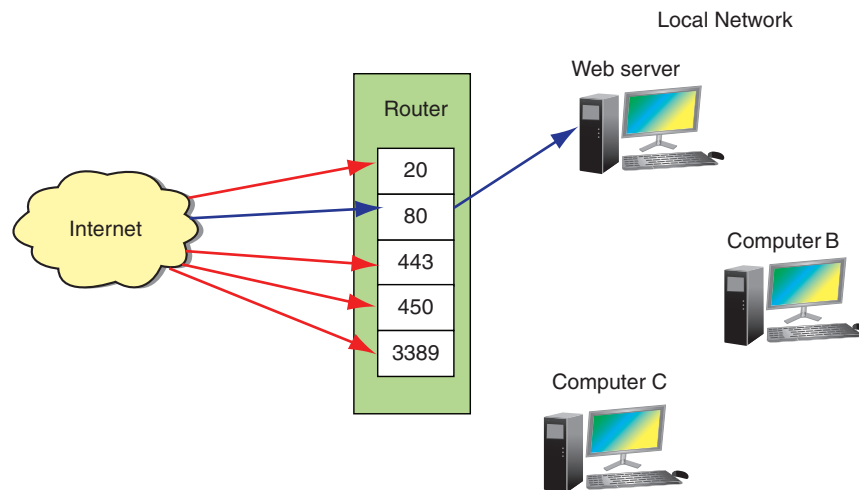
Recall from Chapter 17 that a router can use NAT redirection to present its own IP address to the Internet in place of IP addresses of computers on the local network. The NAT protocol is also responsible for passing communication to the correct port on the correct local computer.



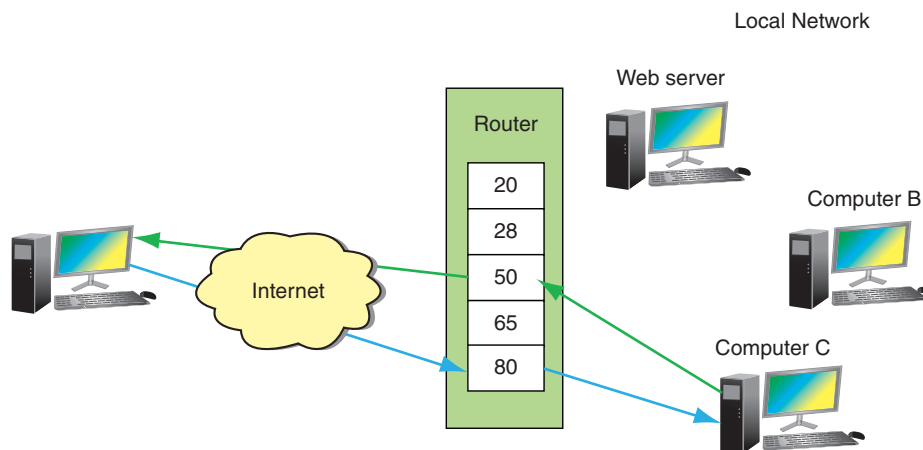
A+  
220-702  
3.2

Here are the ways a device using NAT can protect your network using ports:

- ▲ **Port filtering** is used to open or close certain ports so they can or cannot be used. Remember that applications are assigned these ports. Therefore, in effect, you are filtering or controlling what applications can or cannot be used across the firewall. For example, in Figure 18-37a, all requests from the Internet to ports 20, 443, 450, and 3389 are filtered. These ports are closed.
- ▲ **Port forwarding** means that when the firewall receives a request for communication from the Internet to a specific computer and port, the request will be allowed and forwarded to that computer on the network. The computer is defined to the router by its static IP address. For example, in Figure 18-37a, port 80 is open and requests to port 80 are forwarded to the Web server that is listening at that port. This one computer on the network is the only one allowed to receive requests at port 80.
- ▲ **Port triggering** opens a port when a PC on the network initiates communication through another port. For example, in Figure 18-37b, Computer C sends data to port 50 to a computer on the Internet. The router is configured to open port 80 for



a. Port filtering and port forwarding



b. Port triggering

**Figure 18-37** Port filtering, port forwarding, and port triggering  
Courtesy: Course Technology/Cengage Learning

communication from this remote computer. Port 80 is closed until this trigger occurs. Port triggering does not require a static IP address for the computer inside the network and any computer can initiate port triggering. The router will leave port 80 open for a time. If no more data is received from port 50, then it closes port 80.

**A+ Tip**

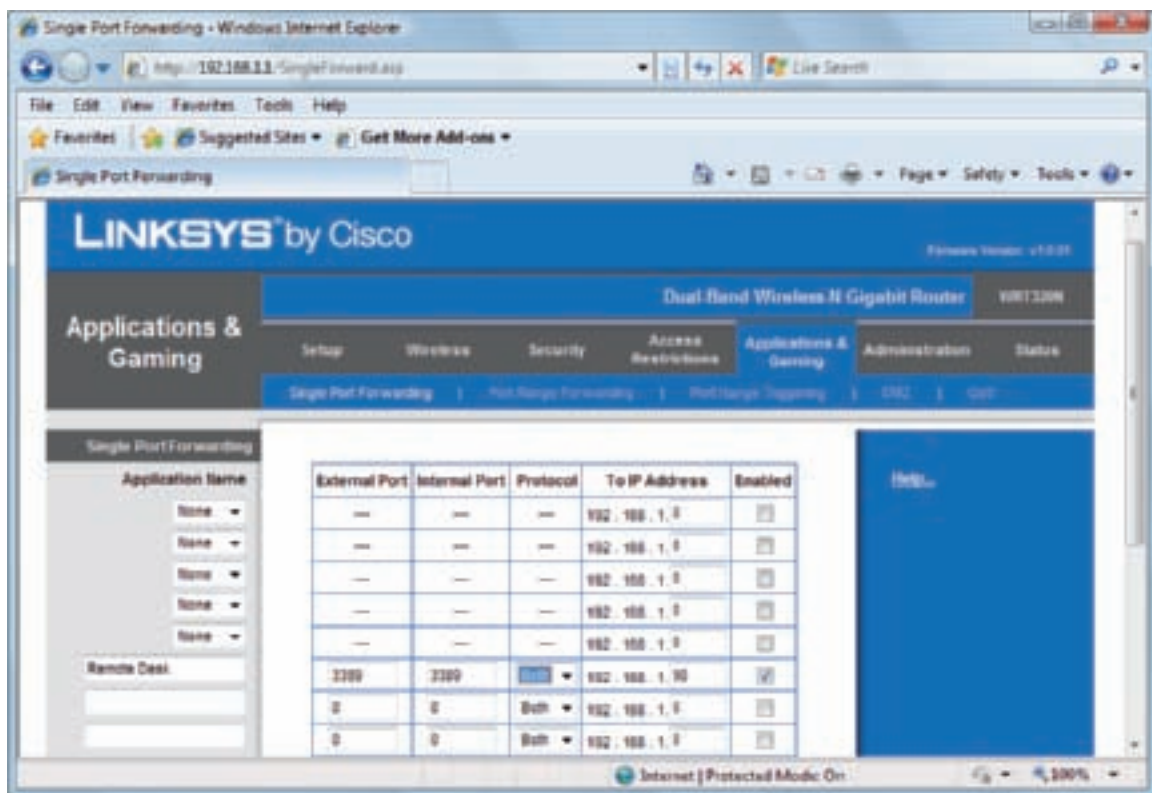
The A+ 220-702 Practical Application exam expects you to know how to implement port forwarding and port triggering.

To configure port forwarding or port triggering, use the Applications & Gaming tab shown in Figure 18-38. In the figure, the Remote Desktop application outside the network can use port forwarding to communicate with the computer whose IP address is 192.168.1.90 using port 3389. The situation is illustrated in Figure 18-39. This computer is set to support the Remote Desktop server application. Later in the chapter, you will learn to use Remote Desktop.

To configure port triggering, click the **Port Triggering** tab and enter the two ranges of ports. For example, in Figure 18-40, the Triggered Range of ports will trigger the event to open the ports listed under Forwarded Range.

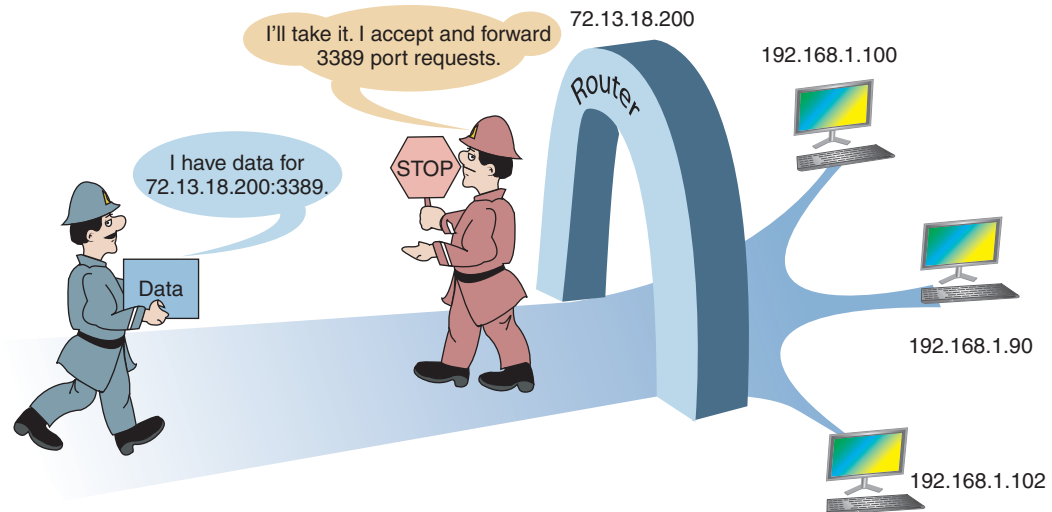
Here are some tips to keep in mind when using port forwarding or port triggering:

- ▲ You must lease a static IP address from your ISP so that people on the Internet can find you. Most ISPs will provide you a static IP address for an additional monthly fee.
- ▲ For port forwarding to work, the computer on your network must have a static IP address so that the router knows where to send the communication.

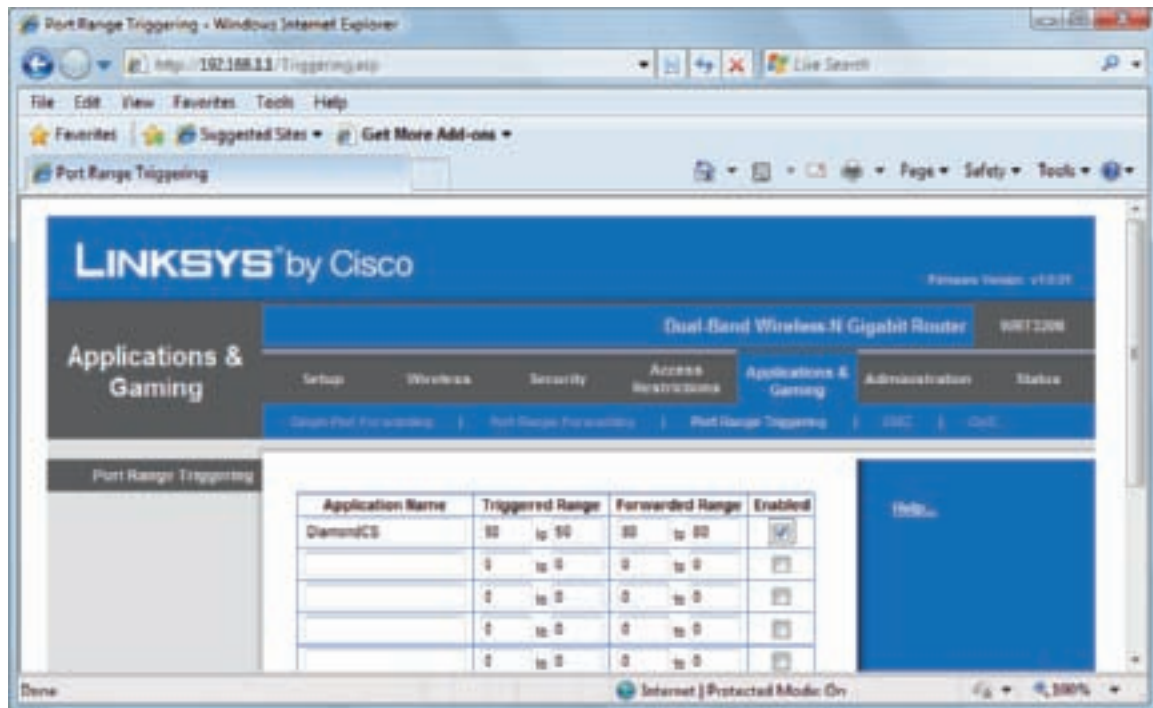


**Figure 18-38** Using port forwarding, you can program your router to allow activity from the Internet to initiate a session with a computer inside the network on a certain port using a static IP address  
Courtesy: Course Technology/Cengage Learning

A+  
220-702  
3.2



**Figure 18-39** With port forwarding, a router allows requests initiated outside the network  
Courtesy: Course Technology/Cengage Learning



**Figure 18-40** Port triggering opens a range of ports when data is sent from inside the network  
Courtesy: Course Technology/Cengage Learning

- ▲ If the computer using port triggering stops sending data, the router might close the triggered port before communication is complete. Also, if two computers on the network attempt to trigger the same port, the router will not allow data to pass to either computer.
- ▲ Be aware that when you use port forwarding or port triggering, your network is more vulnerable because you are allowing external users directly into your private network. For better security, turn on port forwarding only when you know it's being used. In addition, make sure the computer that is receiving outside communication is using a software firewall (for example, Windows Firewall) and antivirus software. In fact, to be on the safe side, recognize that every computer on your network is more vulnerable and be careful to secure each one.

**Tip**

By the way, if you want to use a domain name rather than an IP address to access a computer on your network from the Internet, you'll need to purchase the domain name and register it in the Internet name space to associate it with your static IP address assigned by your ISP. Several Web sites on the Internet let you do both; one site is by Network Solutions at [www.networksolutions.com](http://www.networksolutions.com).

## HOW TO SET UP A WIRELESS NETWORK

Some desktop computers come equipped with a wireless adapter, such as the one in Chapter 17 in Figure 17-16b, that can be configured as a client on a wireless network or as the access point of a wireless network. A wireless access point can also be a stand-alone device such as the one in Figure 18-41 by D-Link. The device supports 802.11g/n and contains a four-port Gigabit switch to connect up to four devices to your wired network. An access point can also serve other purposes, such as the Linksys multifunctional router shown earlier in Figure 18-29. When selecting a wireless access point, consider the 802.11 standards it supports and the security standards it uses. Recall from Chapter 17 that security standards include disabling SSID broadcasting, WPA or WPA2 encryption (or perhaps the outdated WEP encryption), and MAC address filtering.



**Figure 18-41** Xtreme N Duo Wireless Bridge/Access Point by D-Link  
Photo Courtesy of D-Link Systems, Inc.

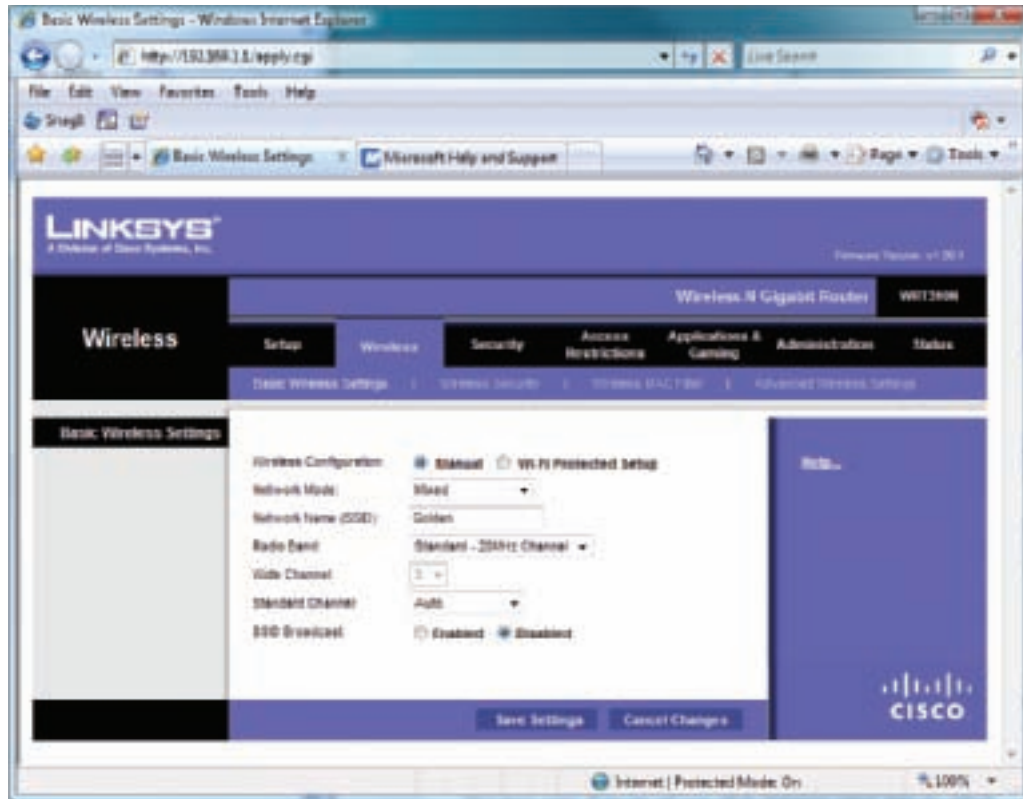
**A+ Tip**

The A+ 220-702 Practical Application exam expects you to know how to install and configure a wireless network, including how to implement wireless security. You need to know how to configure WEP, WPA, SSID, MAC filtering, and DHCP settings.

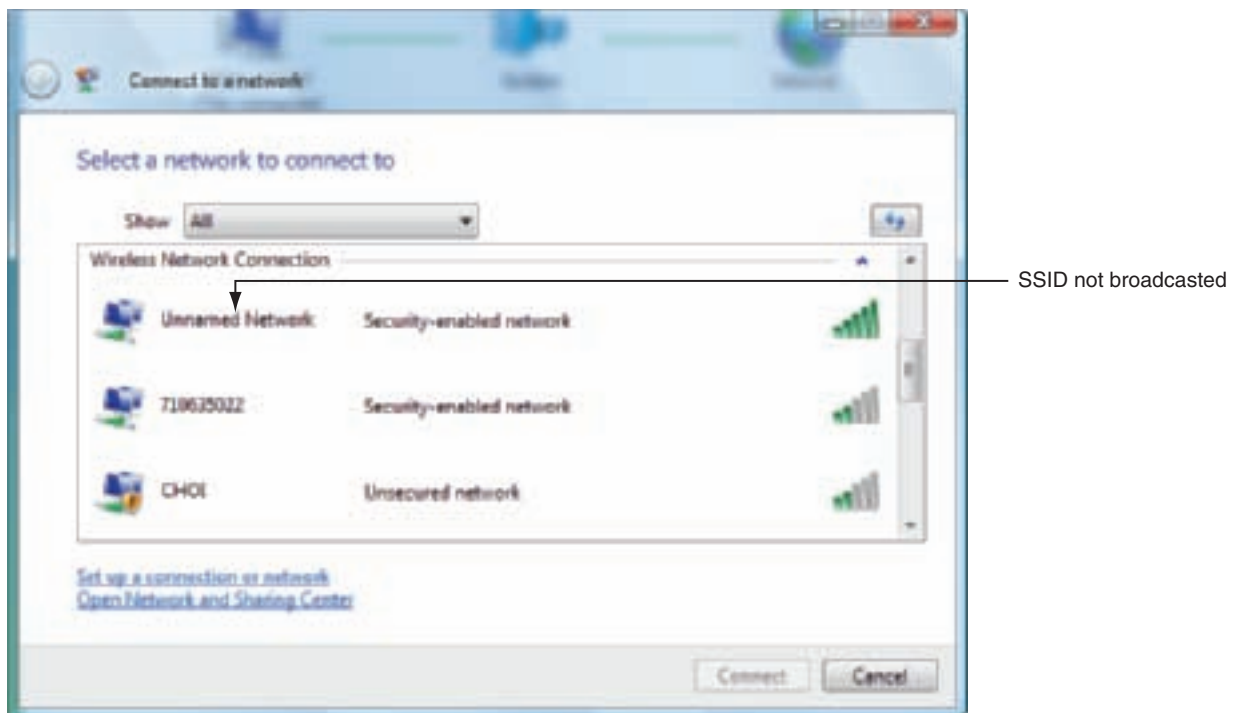
To install a stand-alone access point, position it in the center of where you want your hotspot, and plug it in. It will have a network port to connect to a wired network or a USB port to connect to a computer. Using one of these ports, connect the access point to a computer so that you can configure the access point. If the access point is bundled with a setup CD, run the setup program to step you through the installation. To configure the access point, open a browser and enter the IP address of the access point. Firmware on the device displays the configuration utility. Using this utility, look for ways to change these settings:

1. Look for a way to select the channel the access point will use, the ability to change the SSID of the access point, and the ability to disable SSID broadcasting. Figure 18-42 shows these three settings for a multipurpose Linksys access point. Figure 18-43 shows how a wireless computer sees a wireless access point that is not broadcasting its SSID. This computer would not be able to use this access point until you entered the SSID in the configuration window shown in Figure 18-44.

A+  
220-702  
3.2



**Figure 18-42** Look for the ability of the access point to disable SSID broadcasting  
 Courtesy: Course Technology/Cengage Learning




**Figure 18-43** A wireless computer shows it has located three access points, but the first one listed is not broadcasting its SSID  
 Courtesy: Course Technology/Cengage Learning



**Figure 18-44** Enter the SSID of a wireless network that is not broadcasting its SSID  
Courtesy: Course Technology/Cengage Learning

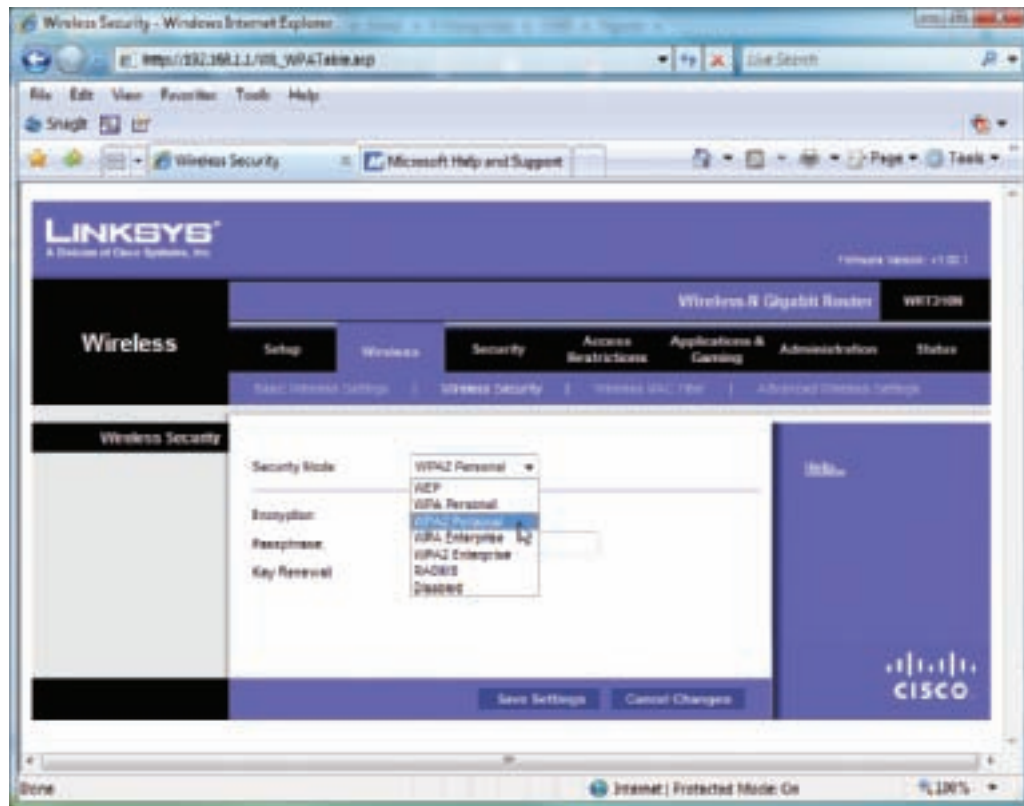
2. To configure data encryption on your access point, look for a wireless security screen similar to the one in Figure 18-45 where you can choose between several WEP, WPA, or RADIUS encryption methods. (RADIUS stands for Remote Authentication Dial-In User Service and uses an authentication server to control access.) WPA2 Personal is the one to choose unless one of your wireless adapters doesn't support it. Enter the passphrase for encryption on this same access point screen. When you connect a PC to this network, you'll need to enter the same passphrase.

 **Notes** To make the strongest password or passphrase, use a random group of numbers, uppercase and lowercase letters, and, if allowed, at least one symbol. Also use at least eight characters in the password.

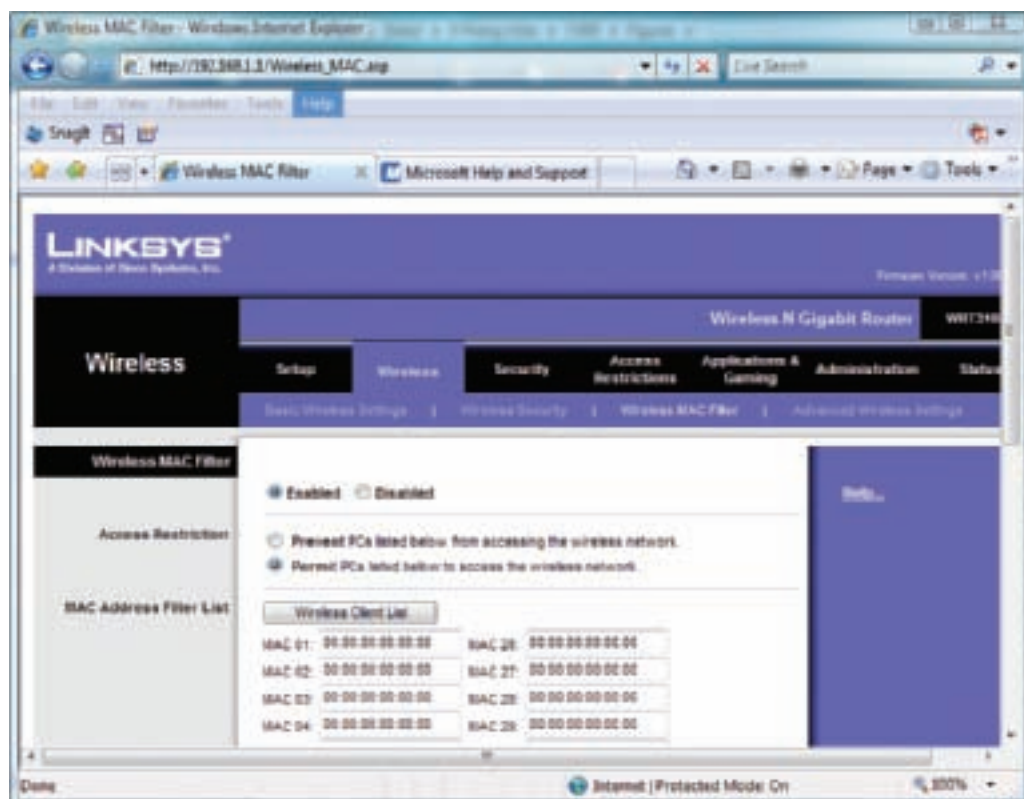
3. Look for MAC filtering on your access point, similar to the screen in Figure 18-46. On this access point, you can enter a table of MAC addresses and decide if this list of MAC addresses is to be used to prevent or permit use of the access point.
4. Decide if your access point will serve up IP addresses (dynamic IP addressing) or if computers that connect to the access point will use static IP addresses. Dynamic IP addressing is the likely choice. To set that up, enable DHCP and set the number of IP addresses that can be used at any one time (which limits the number of computers that can use the wireless network). Also set the beginning IP address. The best choice is to begin with an IP address in the range of 192.168.x.x, so that your network will use private IP addresses. If you want to use static IP addressing on the wireless network, then disable DHCP.
5. Save all your settings for the access point and test the connection. To test it, on one of your wireless computers, follow directions given in Chapter 17 to connect to a hotspot, entering the passphrase when requested. If you don't see the network in the list of wireless networks, try moving your access point or the computer. If you still can't get a connection, remove all security measures and try again. Then restore the security features one at a time until you discover the one causing the problem.



A+  
220-702  
3.2



**Figure 18-45** This wireless access point supports several encryption methods  
Courtesy: Course Technology/Cengage Learning



**Figure 18-46** Configure how the access point will filter MAC addresses  
Courtesy: Course Technology/Cengage Learning



A+  
220-702  
3.2

We've just configured your wireless access point to use several security features. Is it really necessary to use them all? Well, not really. Encryption is essential to keep others from hacking into your wireless data and to prevent unauthorized use of your wireless LAN. For most situations, that's all you need. For added protection, you can disable SSID broadcasting or filter MAC addresses.

## TOOLS AND UTILITIES FOR SUPPORTING AND TROUBLESHOOTING NETWORKS

When supporting and troubleshooting small networks, you'll need to use cable testers to test the physical connections of the network and several TCP/IP utilities to test TCP/IP connectivity. In addition, Remote Desktop and Remote Assistance can be a great help when supporting networks and their users. In this part of the chapter, you'll learn how to use all these tools.

A+  
220-702  
1.4

### CABLE TESTERS

A cable tester can be used to test a cable to find out if it is good or to find out what type of cable it is if the cable is not labeled. You can also use a cable tester to trace a network cable through a building. A cable tester has two components, as shown in Figure 18-47.



**Figure 18-47** Use a cable tester pair to determine the type of cable and if the cable is good  
Courtesy: Course Technology/Cengage Learning

To test a cable, connect each component to the ends of the cable and turn on the tester. Lights on the tester will show you if the cable is good and what type of cable you have. You'll need to read the user manual that comes with the cable tester to know how to interpret the lights.

You can also use cable testers to trace a network cable through a building. Suppose you see several network jacks on walls in a building, but you don't know which jacks connect. Install a short cable in each of two jacks and then use the cable tester to test the continuity, as shown in Figure 18-48. You might damage a cable tester if you connect it to a live circuit, so before you start connecting the cable tester to wall jacks, be sure that you turn off all devices on the network.

A+  
220-702  
1.4



**Figure 18-48** Use cable testers to trace network cables through a building  
Courtesy: Course Technology/Cengage Learning

A+  
220-702  
2.1

## TCP/IP UTILITIES

The TCP/IP component of Windows includes several utilities that can be used to troubleshoot problems with TCP/IP. The most commonly used TCP/IP utilities are Ping and Ipconfig, which you learned about in the last chapter. Table 18-1 lists these and other TCP/IP utilities, and lists the purpose for each. Most of these program files are found in the \Windows\System32 folder.



### A+ Exam Tip

The A+ 220-702 Practical Application exam expects you to know about the following TCP/IP utilities listed in Table 18-2: Ipconfig, Ping, Net, Netstat, Tracert, Nslookup, and Telnet. You need to know when and how to use each utility, and you must be able to interpret results.

Now let's see how to use the Nslookup, Tracert, and Net utilities.

## THE NSLOOKUP COMMAND

Nslookup lets you read information from the Internet name space by requesting information about domain name resolutions from the DNS server's zone data. Zone data is information about domain names and their corresponding IP addresses kept by a DNS server. For example, to find out what your DNS server knows about the domain name `www.microsoft.com`, use this command:

```
nslookup www.microsoft.com
```

Utility	Description
Getmac	Displays the NIC's MAC address (not available in Windows 2000).
Ipconfig	<p>Displays the IP address of the host and other configuration information. (A command used by UNIX similar to Ipconfig is ifconfig.)</p> <ul style="list-style-type: none"> <li>▲ To display all information about connections: <code>ipconfig /all</code></li> <li>▲ To release the current IP address: <code>ipconfig /release</code></li> <li>▲ To request a new IP address: <code>ipconfig /renew</code></li> <li>▲ To display information about Ipconfig: <code>ipconfig /?</code></li> </ul>
Net /?	Get information about the Net command.
Net use	Displays a list of network connections.
Netstat	Displays information about current TCP/IP connections.
Nslookup	Displays information about domain names and their IP addresses.
Ping	<p>Verifies that there is a connection on a network between two hosts. Here are variations of Ping:</p> <ul style="list-style-type: none"> <li>▲ To test for name resolution: <code>ping -a 69.32.142.109</code></li> <li>▲ To continue testing until interrupted: <code>ping -t 69.32.142.109</code></li> <li>▲ To test with a data packet that is 1000 bytes in size: <code>ping -l 1000 69.32.142.109</code></li> </ul>
Telnet	Allows you to communicate with another computer on the network remotely, entering commands to control the remote computer. The connection is not secured.
Tracert	Traces and displays the route taken from the host to a remote destination; Tracert is one example of a trace-routing utility.

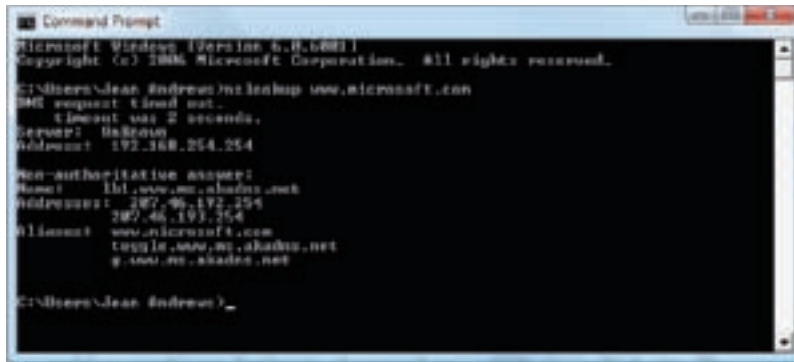
**Table 18-1** TCP/IP utilities available with Windows

Figure 18-49 shows the results. Notice in the figure that the DNS server knows about two IP addresses assigned to `www.microsoft.com`. It also reports that this information is nonauthoritative, meaning that it is not the authoritative, or final, name server for the `www.microsoft.com` computer name.

A **reverse lookup** is when you use the Nslookup command to find the host name when you know a computer's IP address, such as:

```
nslookup 192.168.1.102
```

A+  
220-702  
2.1



```

Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Jean Andrews>nslookup www.microsoft.com
DNS request timed out.
    timeout was 2 seconds.
Server: 8.8.8.8
Address: 192.168.254.254

Non-authoritative answer:
Name:    hl.www.ms.akadns.net
Address: 207.46.193.254
Address: 207.46.193.254
Name:    www.microsoft.com
        toggle.www.ms.akadns.net
        y.www.ms.akadns.net

C:\Users\Jean Andrews>_

```

**Figure 18-49** The Nslookup command reports information about the Internet name space  
Courtesy: Course Technology/Cengage Learning

## THE TRACERT COMMAND

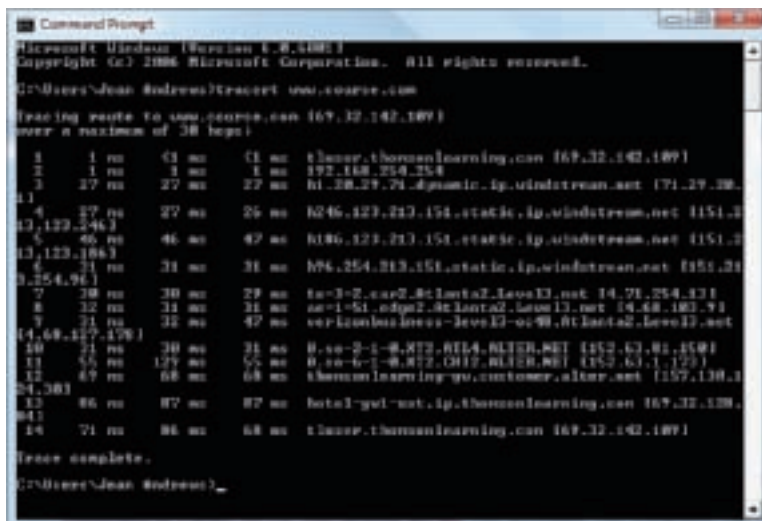
The Tracert (trace route) command can be useful when you're trying to resolve a problem reaching a destination host such as an FTP site or Web site. The command sends a series of requests to the destination computer and displays each hop to the destination. For example, to trace the route to the *www.course.com* site, enter this command in a command prompt window:

```
tracert www.course.com
```

The results of this command are shown in Figure 18-50. By default, the command makes 30 requests for up to 30 hops. The final 15 requests in the figure were not needed to show the complete path to the site, causing a “Request timed out” message to appear. Also, the Tracert command depends on ICMP information sent by routers when a packet's hop count has been exceeded (see Figure 18-51). Some routers don't send this information. If a router doesn't respond, the “Request timed out” message appears.

## THE NET COMMAND

The Net command is several commands in one. These options are Net accounts, Net computer, Net config, Net continue, Net file, Net group, Net help, Net helpmsg, Net localgroup,



```

Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Jean Andrews>tracert www.course.com

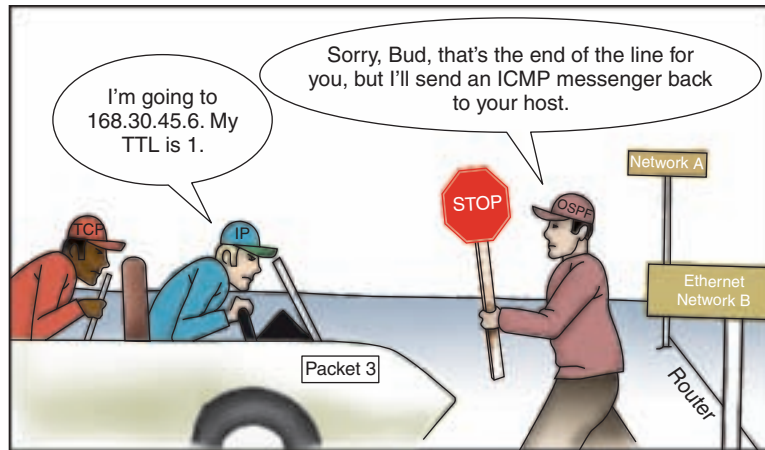
Tracing route to www.course.com [67.32.142.189]
over a maximum of 30 hops:
  0  0 ms  0 ms  0 ms  0 ms  0 ms  0 ms  0 ms  0 ms  0 ms  0 ms  0 ms  0 ms  0 ms  0 ms  0 ms
  1  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms
  2  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms  1 ms
  3  17 ms 17 ms 17 ms 17 ms 17 ms 17 ms 17 ms 17 ms 17 ms 17 ms 17 ms 17 ms 17 ms 17 ms
  4  27 ms 27 ms 27 ms 27 ms 27 ms 27 ms 27 ms 27 ms 27 ms 27 ms 27 ms 27 ms 27 ms 27 ms
  5  46 ms 46 ms 46 ms 46 ms 46 ms 46 ms 46 ms 46 ms 46 ms 46 ms 46 ms 46 ms 46 ms 46 ms
  6  31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms
  7  38 ms 38 ms 38 ms 38 ms 38 ms 38 ms 38 ms 38 ms 38 ms 38 ms 38 ms 38 ms 38 ms 38 ms
  8  32 ms 32 ms 32 ms 32 ms 32 ms 32 ms 32 ms 32 ms 32 ms 32 ms 32 ms 32 ms 32 ms 32 ms
  9  31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms
 10  31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms 31 ms
 11  56 ms 56 ms 56 ms 56 ms 56 ms 56 ms 56 ms 56 ms 56 ms 56 ms 56 ms 56 ms 56 ms 56 ms
 12  49 ms 49 ms 49 ms 49 ms 49 ms 49 ms 49 ms 49 ms 49 ms 49 ms 49 ms 49 ms 49 ms 49 ms
 13  86 ms 86 ms 86 ms 86 ms 86 ms 86 ms 86 ms 86 ms 86 ms 86 ms 86 ms 86 ms 86 ms 86 ms
 14  71 ms 71 ms 71 ms 71 ms 71 ms 71 ms 71 ms 71 ms 71 ms 71 ms 71 ms 71 ms 71 ms 71 ms

Trace complete.

C:\Users\Jean Andrews>_

```

**Figure 18-50** The Tracert command traces a path to a destination computer  
Courtesy: Course Technology/Cengage Learning



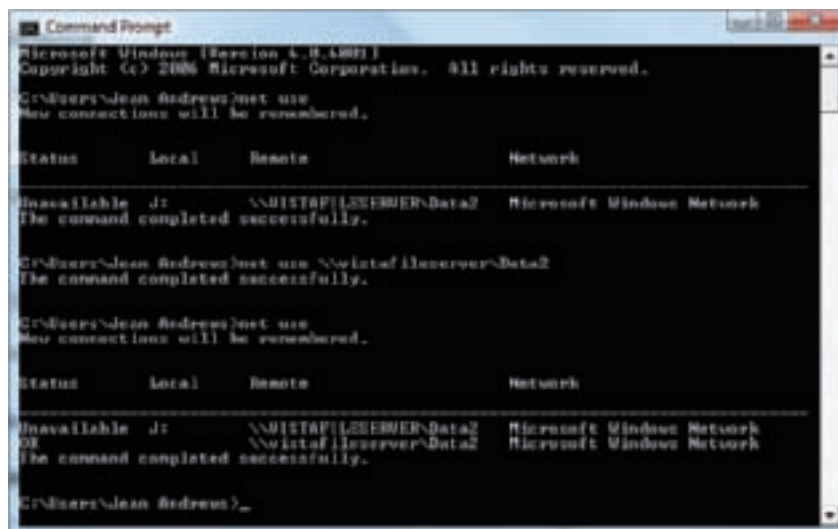
**Figure 18-51** A router eliminates a packet that has exceeded its TTL  
Courtesy: Course Technology/Cengage Learning

Net pause, Net print, Net session, Net share, Net start, Net statistics, Net stop, Net time, Net use, Net user, and Net view.

For example, the Net use command can make a connection to a remote computer, break a connection, or display information about all network connections. Figure 18-52 shows three Net use commands. Here is an explanation of how these commands work:

1. The first command (net use) displays current network connections. You can see that a connection to \\Vistafiler\server\Data2 was attempted in order to create a network drive map to drive J:. (A network drive map makes a folder or volume on a remote computer appear as a local drive, such as J:.) The command to map the drive completed, but the server was not available.
2. The second command (net use \\Vistafiler\server\Data2) made an attempt to connect to the same resource.
3. The third command (net use) shows the connection to \\Vistafiler\server\Data2 is good.

You'll learn to use other variations of the Net command later in the chapter under "Problems with TCP/IP, the OS, and ISP Connectivity."

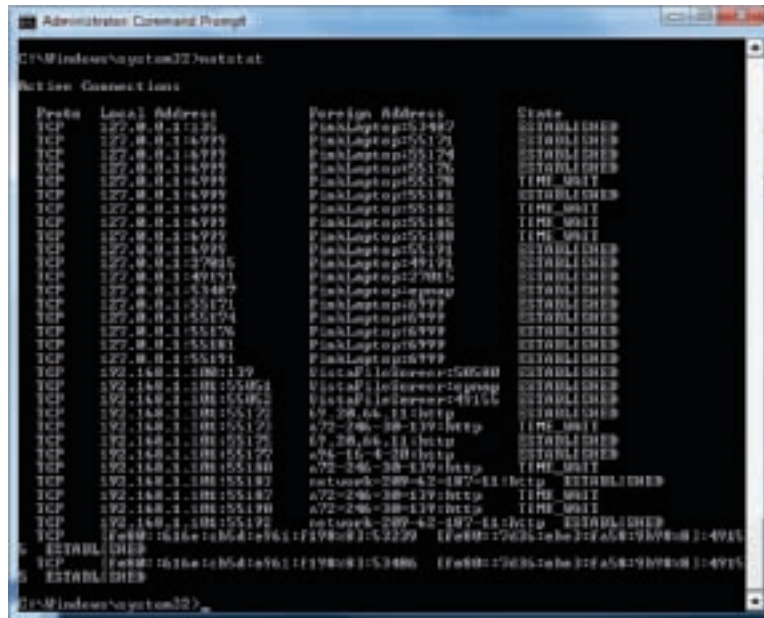


**Figure 18-52** The Net use commands view and make network connections  
Courtesy: Course Technology/Cengage Learning

A+  
220-702  
3.1

## THE NETSTAT COMMAND

The Netstat command gives statistics about network activity (see Figure 18-53) and includes several parameters. One of the most useful is the `-b` parameter that displays the program making the connection. When you use the `-b` parameter, an elevated command prompt is required for Vista. Use the parameter to find malware that might be using your PC for communication on the network or Internet.



**Figure 18-53** Results of a netstat command  
Courtesy: Course Technology/Cengage Learning

To get the best information with the `-b` parameter, include a number, which tells the command to continue until manually interrupted and also send the output to a text file. For example, to collect information every five seconds and log output to the `C:\netstatlog.txt` file, use this command:

```
netstat -b 5 >> C:\netstatlog.txt
```

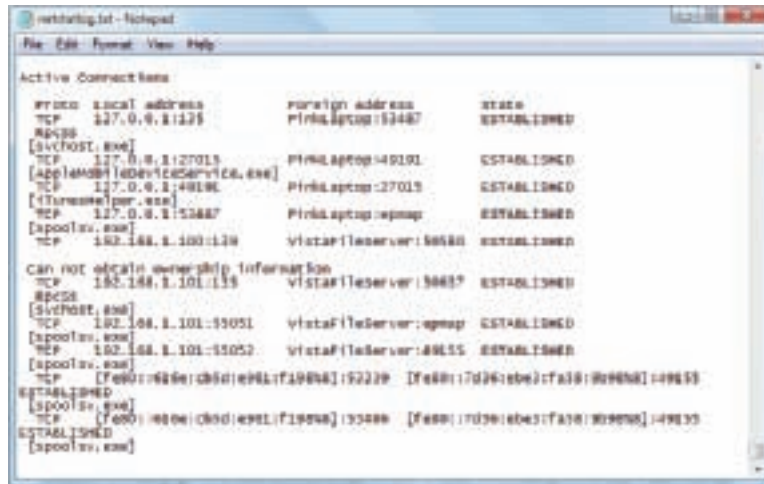
To stop the netstat command, press Ctrl-Break and then check the `C:\netstatlog.txt` file for suspicious activity. The use of the command can also help when trying to find programs that are not malware, but are simply using up networking resources (see Figure 18-54).

A+  
220-702  
3.1  
2.3

## REMOTE DESKTOP

**Remote Desktop** gives a user access to his or her Windows desktop from anywhere on the Internet. As a software developer, I find Remote Desktop extremely useful when I work from a remote location (my home office) and need to access a corporate network to support software on that network. Using the Internet, I can access a file server on these secured networks to make my software changes. It's easy to use and relatively safe for the corporate network. To use Remote Desktop, the computer you want to remotely





**Figure 18-54** Record results to a log file to watch for programs using networking resources  
Courtesy: Course Technology/Cengage Learning

access (the server) must be running Vista Business or Ultimate editions or Windows XP Professional, but the computer you're using to access it (the client) can be running any version of Windows.



#### A+ Tip

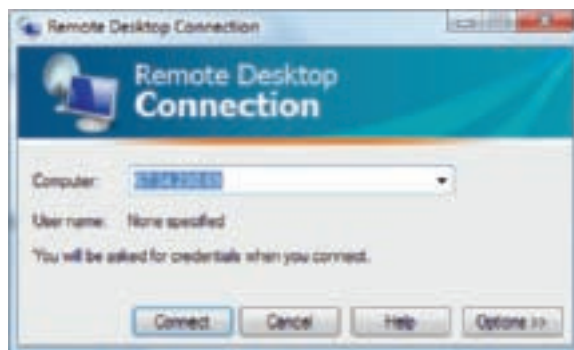
The A+ 220-702 Practical Application exam expects you to know how to use Remote Desktop.

In this section, you'll first see how Remote Desktop can be used, and then you'll see how to set it up for first use.

## HOW REMOTE DESKTOP WORKS

Follow these steps to use Remote Desktop:

1. For Vista, click **Start, All Programs, Accessories and Remote Desktop Connection**. For XP, click **Start, All Programs, Accessories, Communications, and Remote Desktop Connection**. (After Service Pack 3 is applied to Windows XP, the location of Remote Desktop on the Start menu might change to **Start, All Programs, Accessories**.) The Remote Desktop Connection window opens (see Figure 18-55).



**Figure 18-55** Enter the IP address of the remote computer to which you want to connect  
Courtesy: Course Technology/Cengage Learning

A+  
220-702  
3.1  
2.3

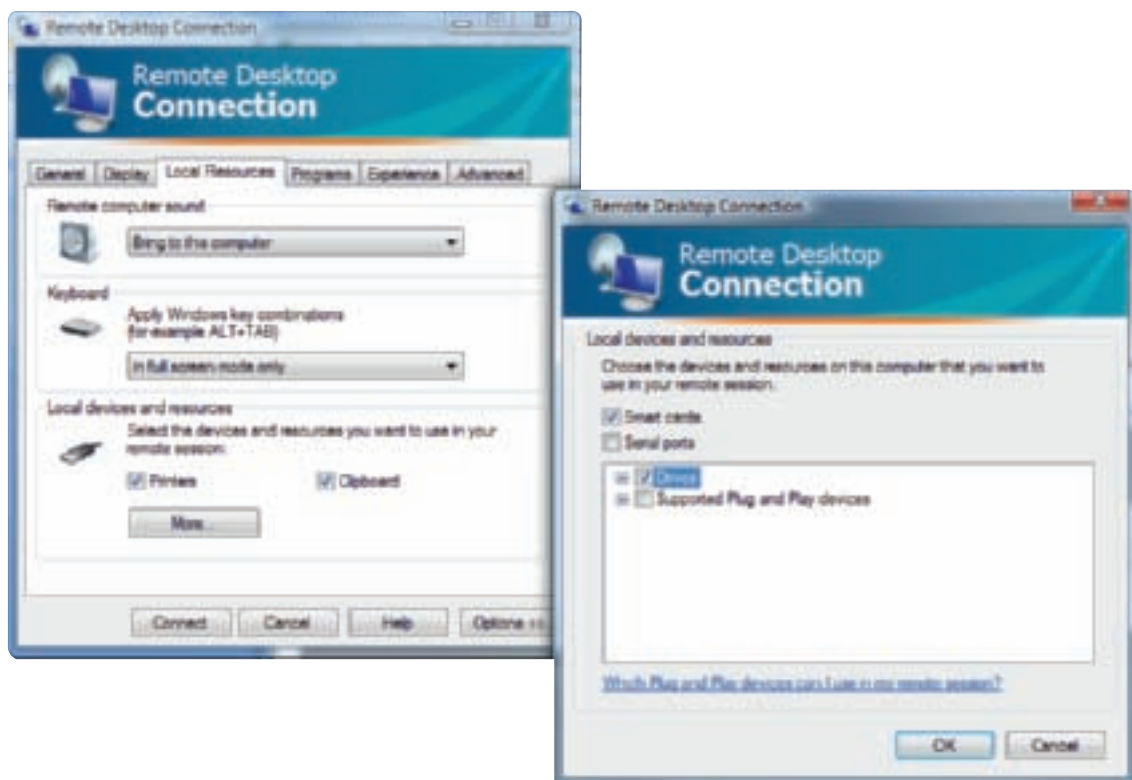
2. Enter the IP address or the host name of the computer to which you want to connect. Begin the host name with two backslashes as in \\VistaFileServer.



### Tip

To use the host name when making a Remote Desktop connection on a local network, the host name and IP address of the remote computer must be entered in the Hosts file of the local computer.

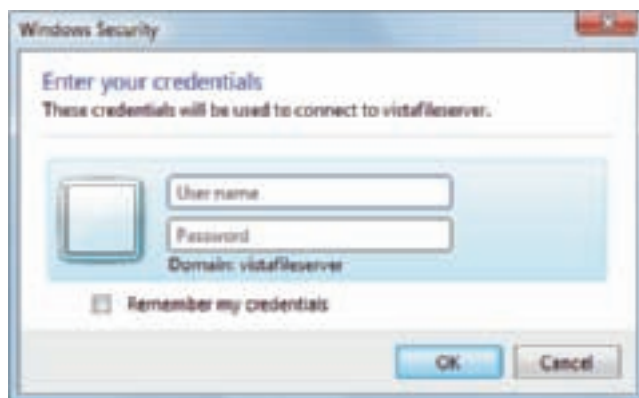
3. If you plan to transfer files from one computer to the other, click **Options** and then click the **Local Resources** tab shown in the left side of Figure 18-56. Click **More**. The box on the right side of Figure 18-56 appears. Check **Drives**. Click **OK**. Click **Connect** to make the connection. Click **Connect** again when a warning box appears. If another warning box appears, click **Yes**.



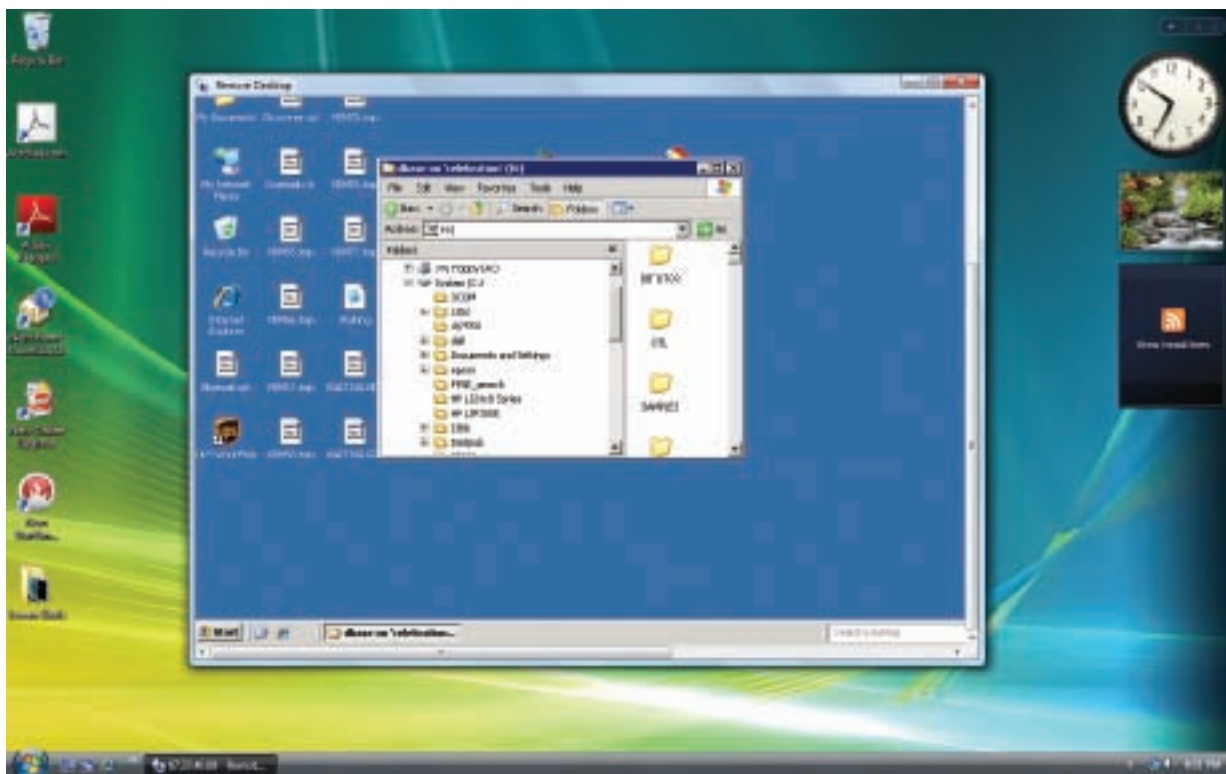
**Figure 18-56** Allow drives and other devices to be shared using the Remote Desktop connection  
Courtesy: Course Technology/Cengage Learning

4. A Windows security box appears that is displayed by the remote computer (see Figure 18-57). Log on using a user name and password for the remote computer.
5. The desktop of the remote computer appears, as shown in Figure 18-58. When you click the desktop, you can work with the remote computer just as if you were sitting in front of it, except response time will be slower. To move files back and forth between computers, use Windows Explorer on the remote computer. Files on your local computer will appear under Network or My Network Places in Windows Explorer on the remote computer. To close the connection to the remote computer, simply close the desktop window.

A+  
220-702  
3.1  
2.3



**Figure 18-57** Enter your user name and password on the remote computer  
Courtesy: Course Technology/Cengage Learning



**Figure 18-58** The desktop of the remote computer is available on your local computer  
Courtesy: Course Technology/Cengage Learning

## HOW TO SET UP REMOTE DESKTOP FOR FIRST USE

To prepare a computer to serve up Remote Desktop, you need to configure the computer for static IP addressing and also configure Remote Desktop for service. Here are the steps needed:

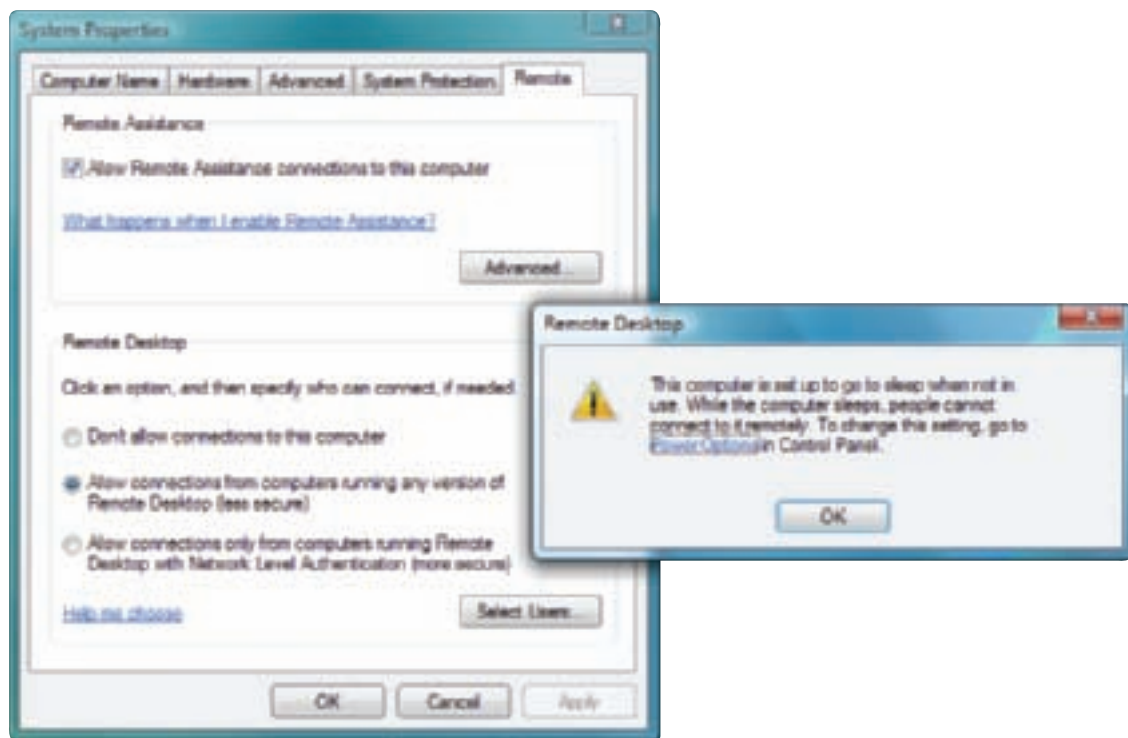
1. As described earlier in the chapter, you'll need a static IP address assigned to you by your ISP. Configure your computer for static IP addressing. If your computer is connected directly to your ISP, assign the IP address given you by your ISP to your computer. If you are using a router on your network, assign your computer a private IP address (for example, 192.168.1.90).

A+  
220-702  
3.1  
2.3

2. If you are using a router on your network, configure the router for port forwarding and allow incoming traffic on port 3389. Forward that traffic to the IP address of your desktop computer. Figure 18-38 shown earlier in the chapter shows one router configured for these settings.
3. Use your browser to verify you have Internet access before you continue to the next steps. If you have a problem, first try repairing your connection and then try rebooting your PC.

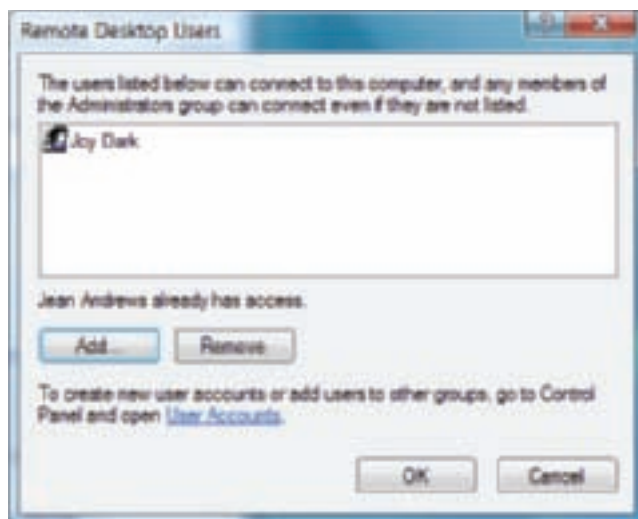
You are now ready to configure Remote Desktop. In the following steps, we are using Windows Vista, but know that the steps in Windows XP work about the same way. Do the following:

1. Click **Start**, right-click **Computer** and select **Properties** from the shortcut menu. Click **Advanced system settings** and respond to the UAC box. The System Properties box appears (see the left side of Figure 18-59). Click the **Remote** tab and check **Allow connections from computers running any version of Remote Desktop (less secure)**. A dialog box might appear warning that the computer is set to go into sleep mode when not in use (see the right side of Figure 18-59). Click **OK** to close the box.



**Figure 18-59** Configure a computer to run the Remote Desktop service  
Courtesy: Course Technology/Cengage Learning

2. Click **Select Users**. In the dialog box that opens (see Figure 18-60), add the users of this computer who will be using Remote Desktop. Users who have administrative privileges will be allowed to use Remote Desktop by default, but other users need to be added. Click **OK** twice to exit both windows.



**Figure 18-60** Add local users who are allowed access by way of Remote Desktop  
Courtesy: Course Technology/Cengage Learning

3. Verify that Windows Firewall is set to allow Remote Desktop activity to this computer. To do that, open the **Network and Sharing Center** and click **Windows Firewall**. Then click **Change settings** and respond to the UAC box. The Windows Firewall Settings box opens. On the **General** tab, verify that Windows Firewall is turned on and that **Block all incoming connections** is *not* selected. Then click the **Exceptions** tab and verify that **Remote Desktop** is checked so that Remote Desktop incoming activity is allowed. Close all windows.
4. You are now ready to test Remote Desktop using your local network. Try to use Remote Desktop from another computer somewhere on your local network. Verify you have Remote Desktop working on your local network before you move on to the next step of testing the Remote Desktop connection from the Internet.
5. If you want Remote Desktop available at all times, use the Power Options window in Control Panel to allow the computer to wake up when it has network activity. How to manage power options is covered in Chapter 21.



**Notes** Even though Windows normally allows more than one user to be logged on at the same time, this is not the case with Remote Desktop. When a Remote Desktop session is opened, all local users are logged off.

Is your computer as safe as it was before you set it to serve up Remote Desktop and enabled port forwarding to it? Actually, no, so take this into account when you decide to use Remote Desktop. In a project at the end of this chapter, you'll learn how you can take further steps to protect the security of your computer when using Remote Desktop.

## REMOTE ASSISTANCE

**Remote Assistance** can help you support users and their computers from a distance. The user who needs your help sends you an invitation by e-mail or chat to connect to her computer using Remote Assistance. When you respond to the invitation, you can see the user's desktop just as she sees it. And, if the user gives you permission, you can take control of her computer



A+  
220-702  
3.1  
2.3

to change settings or do whatever else is needed to fix her problem or show her how to perform a task. Think of Remote Assistance as a way to provide virtual desk-side support.

**A+ Tip**

Assistance.

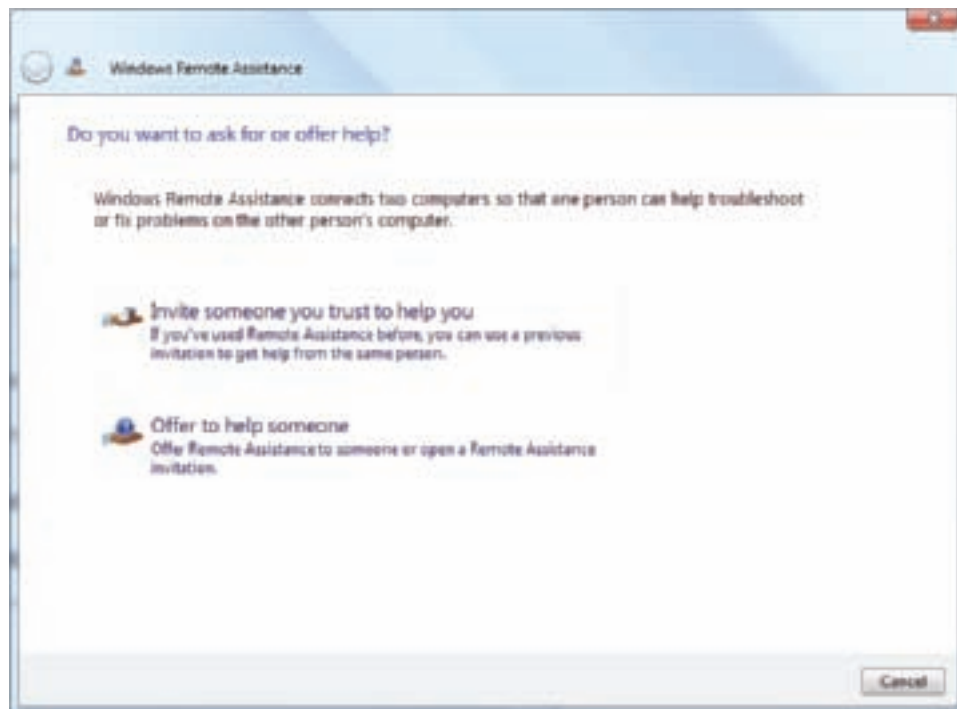
The A+ 220-702 Practical Application exam expects you to know how to use Remote

There are several ways to initiate a Remote Assistance session:

- ▲ The user saves an invitation file and then sends that file to the technician. The file can be sent by any method, including e-mail, chat, or posting to a shared folder on the network. This is the easiest method to start a Remote Assistance session.
- ▲ The user can initiate a session by way of Windows Messenger. This method works well when the user is behind a hardware firewall that the technician must get past.
- ▲ The user can send an e-mail message to a corporate help desk. The e-mail contains an attached file that the technician uses to respond to the invitation. This method works well when both people belong to the same domain and no hardware firewalls are between them.
- ▲ The technician can initiate a session. This method is the most difficult to use, requiring that Group Policies be applied on the technician's computer.

Use the following steps to initiate a Remote Assistance session when the user sends you an invitation. First, ask the user to send you the invitation. When she does so, her computer is set up to respond to Remote Assistance communication. She must do the following:

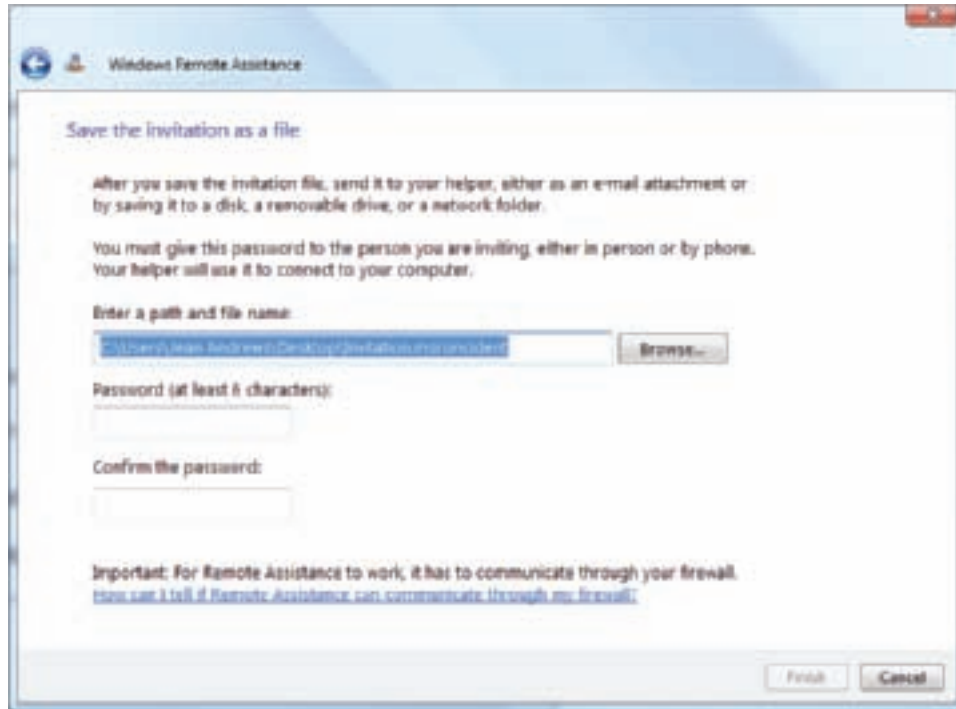
1. Click **Start, Help and Support**. In the Help and Support window, click **Windows Remote Assistance**. The window in Figure 18-61 appears.



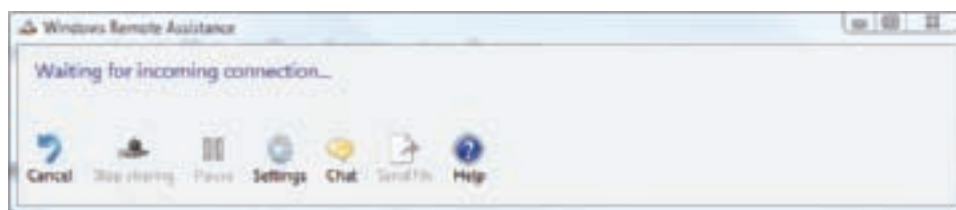
**Figure 18-61** The user can invite someone to help  
Courtesy: Course Technology/Cengage Learning



2. Click **Invite someone you trust to help you**. On the next window, click **Save this invitation as a file**.
3. On the next window (see Figure 18-62), the user verifies the location of the file (the Windows desktop), enters a password, confirms the password, and then clicks **Finish**. The file is created and the Windows Remote Assistance window appears (see Figure 18-63).



**Figure 18-62** The user creates a password for you to use  
Courtesy: Course Technology/Cengage Learning

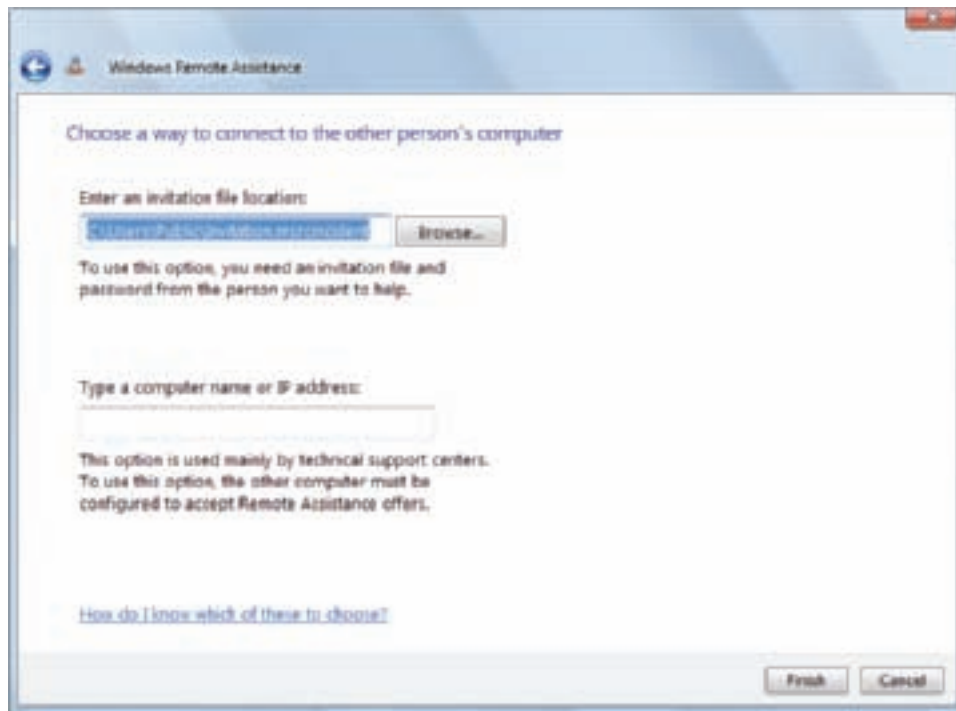


**Figure 18-63** Remote Assistance waiting for incoming connection  
Courtesy: Course Technology/Cengage Learning

The user must send you the invitation file and tell you the password. She can attach it to an e-mail message or chat session or hand it to you on a jump drive. When you have the invitation file and password, follow these steps to accept the invitation:

1. Click **Start, Help and Support**, and click **Windows Remote Assistance**. (Alternately, you can enter **Windows Remote Assistance** in the Vista Start Search box.) On the first box (refer back to Figure 18-61), click **Offer to help someone**. On the second box (see Figure 18-64), click **Browse** and point to the location of the invitation file. Click **Finish**.

A+  
220-702  
3.1  
2.3



**Figure 18-64** Point to the location of the invitation file  
Courtesy: Course Technology/Cengage Learning

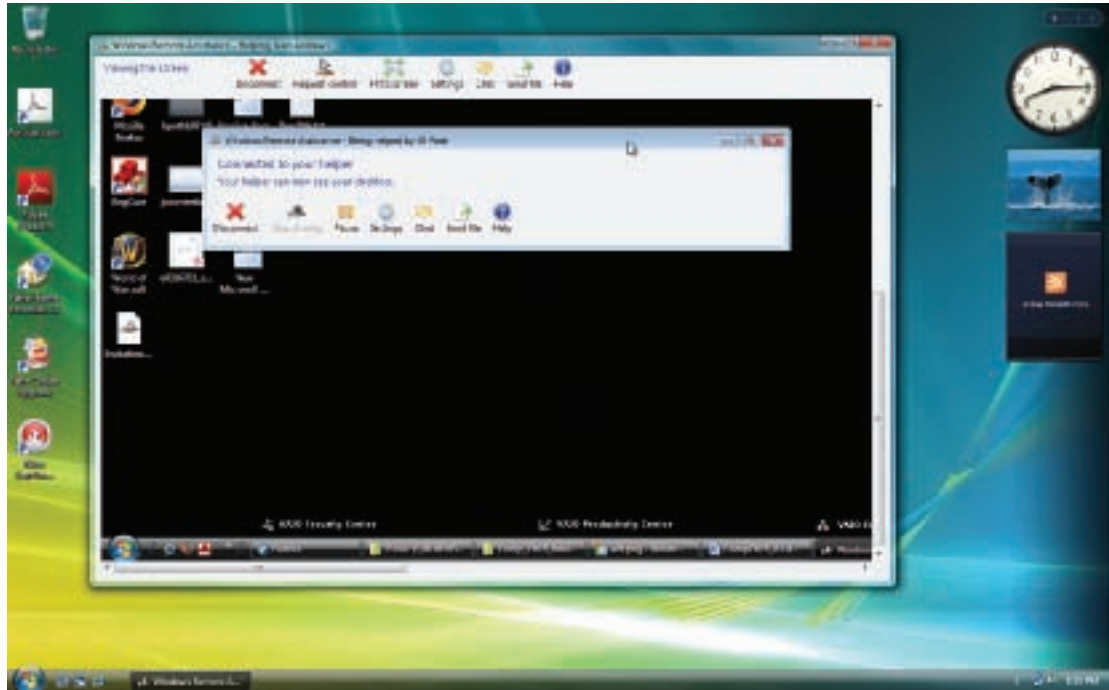
2. On the next box, enter the password given you by the user. Click OK.
3. The user sees the box in Figure 18-65 appear on her desktop. She must click **Yes** to allow you to connect.



**Figure 18-65** The user gives Jill West permission to connect  
Courtesy: Course Technology/Cengage Learning

4. The background of the user's desktop turns black. A window on your desktop opens where you can see the user's desktop (see Figure 18-66). Here are some things you and the user can do so that you can assist the user:
  - ▲ To open a chat session with the user, click the **Chat** icon. A chat pane appears in the Remote Assistance window on both desktops.
  - ▲ To ask the user if you can take control of her desktop, click **Request control** in the Remote Assistance window. When the user accepts the request, you can control her computer.
  - ▲ The user can hide her desktop from you at any time by clicking **Pause** in the control window.

A+  
220-702  
3.1  
2.3



**Figure 18-66** The user's desktop can be viewed by the support technician  
Courtesy: Course Technology/Cengage Learning

- ▲ Either of you can disconnect the session by clicking **Disconnect** in the control window.
- ▲ A log file is kept of every Remote Assistance session in the C:\Users\username\Documents\Remote Assistance Logs folder. The file includes the chat session. If you type instructions during the chat session that will later help the user, she can use the log file to remind her of what was said and done.
- ▲ If an invitation created by a user is not used within six hours, the invitation expires.


If you have problems making the connection, do the following:

1. Windows Firewall on the user's computer might be blocking Remote Assistance. Verify that Remote Assistance is checked as an exception to blocked programs in the Windows Firewall window.
2. If you are outside the user's local network, the hardware firewall protecting her network might be blocking Remote Assistance. Verify that port forwarding on that hardware firewall is enabled for Remote Assistance. Remote Assistance uses port 3389, the same port used by Remote Desktop.

## ***TROUBLESHOOTING NETWORK AND INTERNET CONNECTIONS***

A+  
220-702  
3.1

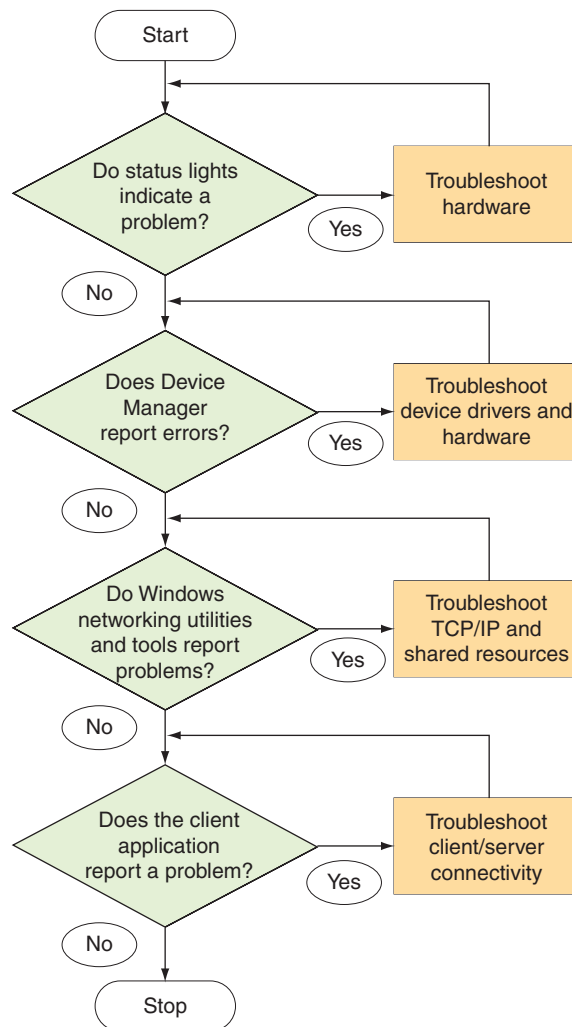
If you have problems connecting to the network, you can follow the flowchart in Figure 18-67 to eliminate hardware, device drivers, the Windows configuration, and applications when troubleshooting network connections. Recall that networking happens in layers. This flowchart reminds us troubleshooting problems with networking starts at the bottom layer (hardware) and proceeds to the top layer (applications).

 **Video**  
Troubleshooting a Network

18

A+ 220-702

A+  
220-702  
3.1



**Figure 18-67** Flowchart to troubleshoot network connections  
Courtesy: Course Technology/Cengage Learning



#### A+ Exam Tip

The A+ 220-702 Practical Application exam expects you to know how to troubleshoot network problems by using cable testers and, checking TCP/IP settings, firewall settings, proxy settings, and protocol settings used within client applications. All these skills are covered in this part of the chapter.

Now let's look at the strategies you can use to troubleshoot network problems, starting first with hardware and then proceeding to TCP/IP settings within Windows, and finally by checking protocol settings used with the client application that is not working.

A+  
220-702  
1.2  
1.4

## PROBLEMS WITH HARDWARE AND DEVICE DRIVERS

When a PC cannot communicate on a network, begin by checking hardware. To verify network hardware and solve problems with hardware, follow these steps:

1. Check the status indicator lights on the NIC or the motherboard Ethernet port. A steady light indicates connectivity and a blinking light indicates activity. If you don't see either light, this problem must be resolved before you consider OS or application problems.

A+  
220-702  
1.2  
1.4

2. Check the network cable connection at both ends. Is the cable connected to a port on the motherboard that is disabled? It might need to be connected to the network port provided by a network card. Check the indicator lights on the router or switch at the other end. Try a different port on the device.
3. For wireless networking, make sure the wireless switch on a laptop is turned on. Move the laptop to a new position in the hotspot. Rebooting a laptop often solves the problem of not receiving a signal.
4. Determine whether other computers on the network are having trouble with their connections. If the entire network is down, the problem is not isolated to the PC you are working on. Check the switch, hub, or router controlling the network.
5. Check the network cable to make sure it is not damaged. If the cable is frayed, twisted, or damaged, replace it. You can also use cable testers to verify the cable is good.
6. When using an Ethernet wall jack to connect the PC to a router or switch in another location in the building, consider that the network cabling in the walls might be bad or not connected to the router or switch at the other end. Disconnect the cable at the wall jack near your PC, and disconnect the cable at the router or switch. Next, use cable testers at both these ends to verify connectivity between the wall jack and the cable near the router or switch.

**A+ Tip**

The A+ 220-702 Practical Application exam expects you to know how and when to use cable testers.

7. Open the computer case and make sure the NIC is securely seated in the expansion slot. Try reseating the card. Reboot and check for activity lights. If you still don't see activity, replace the NIC, and then install new drivers.

To solve problems with device drivers, which might also be related to a problem with the NIC, follow these steps:

1. Make sure the network adapter and its drivers are installed by checking for the adapter in Device Manager. Device Manager should report the device is working with no problems.
2. Try updating the device drivers.
3. Try uninstalling and reinstalling the network adapter drivers. If the drivers still install with errors, try downloading new drivers from the Web site of the network card manufacturer. Also, look on the installation CD that came bundled with the adapter for a setup program. If you find one, uninstall the adapter and run this setup program.
4. Some network adapters have diagnostic programs on the installation CD. Try running the program from the CD. Look in the documentation that came with the adapter for instructions on how to install and run the program.
5. For an onboard network port, update or reinstall drivers provided by the motherboard driver CD or the motherboard Web site manufacturer.
6. If Device Manager still reports errors, try running antivirus software and updating Windows. Then try installing a known-good network adapter. If that does not work, the problem might be a corrupted Windows installation.

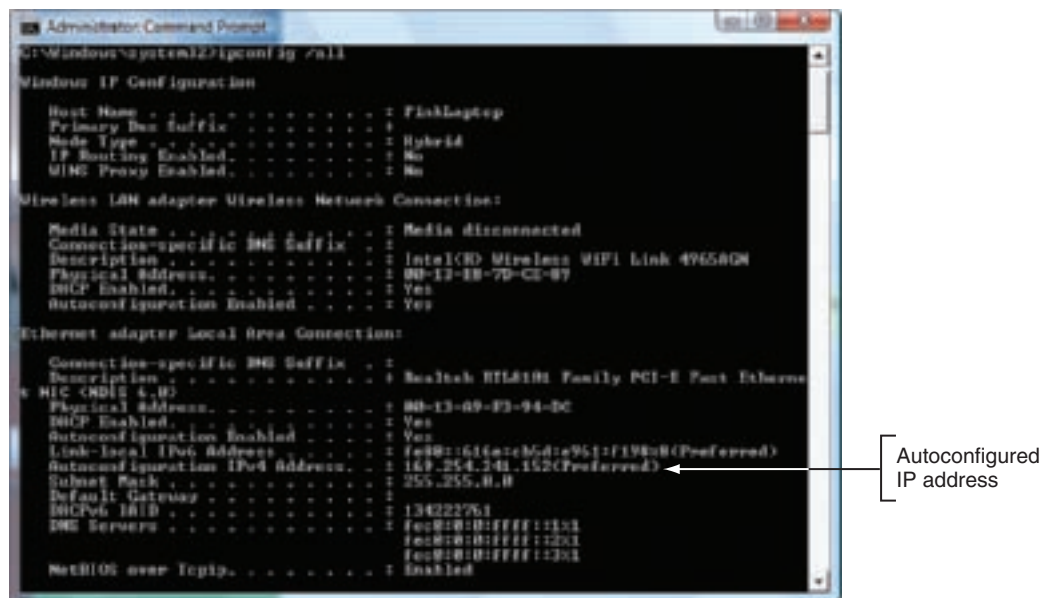
After you have verified the status indicator lights on the NIC and Device Manager recognizes the NIC with no errors, move on to the next step of checking TCP/IP settings.

A+  
220-702  
2.1  
3.1

## PROBLEMS WITH TCP/IP, THE OS, AND ISP CONNECTIVITY

To solve problems with Windows TCP/IP configuration and connectivity, follow these steps to verify that the local computer is communicating over the network:

1. Try to release the current IP address and lease a new address. To do this using Vista, open the Network and Sharing Center window and click **Diagnose and repair**. For XP, in the Network Connections window, right-click the network icon and select **Repair** from the shortcut window. Alternately, you can open a command prompt window and use these two commands: `ipconfig /release` followed by `ipconfig /renew`. (Vista requires an elevated command prompt window.)
2. Look for problems with the TCP/IP configuration. Enter `ipconfig /all` at the command prompt. If the TCP/IP configuration is correct and an IP address is assigned, then the IP address, subnet mask, and default gateway appear along with the MAC address. For dynamic IP addressing, if the PC cannot reach the DHCP server, then it assigns itself an Automatic Private IP Address (APIPA). The `ipconfig` command shows the IP address as the Autoconfiguration IPv4 Address, and the address begins with 169.254 (see Figure 18-68). In this case, suspect that the PC is not able to reach the network or the DHCP server is down.



**Figure 18-68** The network connection was not able to lease an IP address  
Courtesy: Course Technology/Cengage Learning

3. Next, try the loopback address test. At a command prompt, enter the command `ping 127.0.0.1` (with no period after the final 1). This IP address always refers to your local computer. It should respond with a reply message from your computer. If this works, TCP/IP is likely to be configured correctly. If you get an error, then assume that the problem is on your PC. Recheck the installation and configuration of each component, such as the network card and the TCP/IP settings. Remove and reinstall each component, and watch for error messages, writing them down so that you can recognize or research them later as necessary. You might need to uninstall and reinstall the TCP/IP component. Compare the configuration to that of a working PC on the same network.



4. If you're having a problem with slow network performance, suspect a process is hogging network resources. Use the `netstat` command with the `-b` parameter described earlier in the chapter to help you find this program. Netstat can also help you find out if the program you want to use to access the network is actually running.
5. Verify that the software firewall on the PC is not the source of the problem. Is Windows Firewall set correctly? Is a third-party personal firewall blocking communication? ZoneAlarm sometimes gives problems by blocking communication that you want. Try disabling ZoneAlarm. If the connection now works, carefully check all ZoneAlarm settings.

If you are having problems reaching another computer on your network, follow these steps:

1. Open the Vista Network window or the XP My Network Places window. Normally, a computer on the network shows up in these places as an icon. Try to drill down to the shared resources on this computer. Press the F5 key to refresh the window.
2. Now try to ping the host computer you are trying to reach. If it does not respond, then the problem might be with the host computer or with the network to the computer.
3. When trying to reach a computer on your local network, try the Ping command with the IP address of the remote computer. Next, try the Ping command using the computer name of the remote computer. If the Ping command works when using an IP address, but does not work when using a host name on the local network, check the Hosts file on the local computer. Make sure the IP address and host name entry line in the file are correct. The problem might also be with wrong entries in DNS servers that are used on the corporate network. One or more DNS servers might hold an entry that relates the IP address to the wrong host name.
4. These commands can help solve problems with host names on the local network:
  - a. Use the `nslookup` command to find the computer's IP address.
  - b. Try this command: `net view \\computername`. If two computers on the network have the same computer name, the command reports this error. Then change the name of one computer.
5. If you can ping or Net view a computer, but cannot access it in the Network window or My Network Places, verify the computer is in the same domain or workgroup that the local computer is in. Also make sure the remote computer has File and Printer Sharing turned on. Also verify that the user account and password are the same on both computers.
6. Use this command to verify that resources on a remote computer are shared:

```
net view \\computername
```

The command should list the shared resources. If the command gives an error about access being denied, the problem is with permissions. Make sure the account you are using is an account recognized by the remote computer. Try this command to pass a new account to the remote computer:

```
net use \\computername /user:username
```

A+  
220-702  
2.1  
3.1

In the above command, if there is a space in the username, enclose the username in double quotation marks, as in:

```
net use \\computername /user:"Jean Andrews"
```

7. If the net view command using a computer name does not work, try the command using the remote computer's IP address, as in:

```
net view 192.168.1.102
```

If this command works, the problem is likely with name resolution. Make sure the computer name you are using is correct and the computer is in your workgroup or domain.

8. If you're having problems getting a network drive map to work, try making the connection with the net use command like this:

```
net use z: \\computername\folder
```

To disconnect a mapped network drive, use this command:

```
net use z: /delete
```

If you can see resources on the local network, but cannot access the Internet, do the following:

1. Try to ping your default gateway using its IP address. If that doesn't work, move on to Step 5.
2. To eliminate DNS as the problem, follow these steps:
  - a. Try substituting a domain name for the IP address in a ping command:

```
ping www.course.com
```

If this ping works, then you can conclude that DNS works. If an IP address works, but the domain name does not work, the problem lies with DNS.

- b. If DNS is being provided by your ISP and you are using dynamic IP addressing with your ISP, try rebooting the cable modem or DSL modem. Also try this command to flush the DNS cache kept on the computer:

```
ipconfig /flushdns
```

- c. Try pinging your DNS server. To find out the IP address of your DNS server, open the firmware utility of your router and look on a status screen.
  - d. If your ISP is providing you with a static IP address and with IP addresses for DNS servers, you must manually enter these values into your router firmware utility. Contact the ISP and verify the DNS IP addresses you are using are correct. You can find this information in the support section of the ISP Web site.

3. If you're having a problem accessing a particular computer on the Internet, try using the `tracert` command, for example:

```
tracert www.course.com
```

The results show computers along the route that might be giving delays.

4. If one computer on the network cannot access the Internet but other computers can, check the MAC address filtering on the router. Make sure this computer is allowed access. To find out a PC's MAC address, use the `Getmac` or `Ipconfig` command.
5. Perhaps the problem is with your firewall. Verify your firewall settings. Zone Alarm sometimes gives this type of problem. Try disabling Zone Alarm to eliminate it as the problem. To completely disable it, make sure all Zone Alarm services and processes are stopped.
6. If you are not able to access the Internet at all, do the following to recycle the connection to your ISP:
  - a. Turn off the cable modem, DSL modem, or other device that you use to connect to your ISP. Turn off the router.
  - b. Turn back on the cable modem, DSL modem, or other ISP device. Wait until the lights settle. Then turn on your router.
  - c. On any PC on your network, release and renew the IP address. Open your browser and try to browse some Web sites.
7. For a cable modem, check to make sure your television works. The service might be down.
8. Perhaps the problem is with your router or one of its features. Try accessing the Internet without using the router. First configure Windows Firewall on one PC for maximum protection, blocking all uninvited communication. Configure TCP/IP on your PC to match up with what your ISP is using (dynamic or static IP addressing). Then use a network cable to connect this PC directly to your cable modem, DSL modem, or other Internet device. If you can access the Internet, you have proven the problem is with the router or cables going to it. To eliminate the cables as a problem, replace them. Connect the router back up to the PC and check all the router settings. The problem might be with DHCP, the firewall settings, or port forwarding. Try updating the firmware on the router. If you are convinced all settings on the router are correct, but the connection to your ISP works without the router and does not work with the router, it's time to replace the router.
9. If you still cannot access the Internet, contact your ISP.

## PROBLEMS WITH CLIENT-SIDE APPLICATIONS

Problems with client-side applications might be caused by router or firewall settings, secured connections not working, e-mail protocol settings, FTP problems, and VoIP connections. All these concerns are covered next.

## ROUTER AND FIREWALL SETTINGS

When trying to use client/server applications on the Internet, your software and hardware firewalls and other security settings on the router must allow the communication.

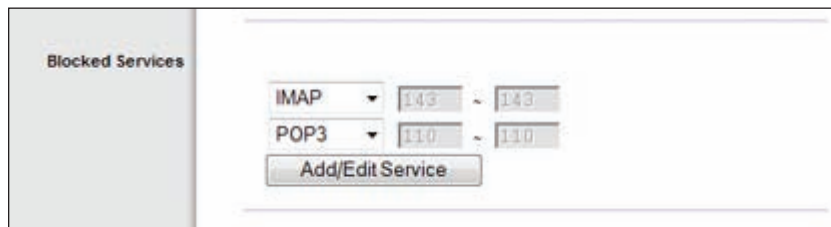
A+  
220-702  
3.1

Open Windows Firewall on the local computer and verify these settings:

1. Following instructions given earlier in the chapter, verify Windows Firewall settings. Make sure Vista Windows Firewall is on and that **Block all incoming connections** is not checked. For XP, verify that **Don't allow exceptions** is not checked.
2. Click the **Exceptions** tab, and make sure the service or program you are trying to use is checked. If you don't see your service or program listed, click **Add program** (refer back to Figure 18-26), select the program from the list of installed programs, and click **OK**. If you know the specific port you want to open, click **Add port** (refer back to Figure 18-26) and enter any name to help you remember the purpose of this port, the port, and protocol (TCP or UDP) on the Add a Port box. Click **OK** to close the box.

If the problem is still not solved, follow these steps to make sure your router is not blocking communication:

1. Verify that NAT redirection settings are correct. Is port forwarding enabled for the specified ports? Is the range of ports correct for this client application? Check the program documentation to find out what range it uses. There might be more than one port or a range of ports. If you can't find the information in the documentation, search the Internet.
2. Is port forwarding set to the correct IP address on the network? Verify the computer is using this IP address. Set the computer for static IP addressing or set the router to always serve up this IP address to this computer.
3. Check the access restrictions screen of the router and make sure restriction policies are not applied. For example, is the router configured to deny service for a certain day of the week or time of day? Is the MAC address or the IP address of the PC in the list of addresses that are denied Internet access? Verify that a service is not blocked. For example, the IMAP and POP3 services are listed under Blocked Services in Figure 18-69. These services are needed to receive e-mail on the network.



**Figure 18-69** Blocked services prevent communication across the firewall  
Courtesy: Course Technology/Cengage Learning

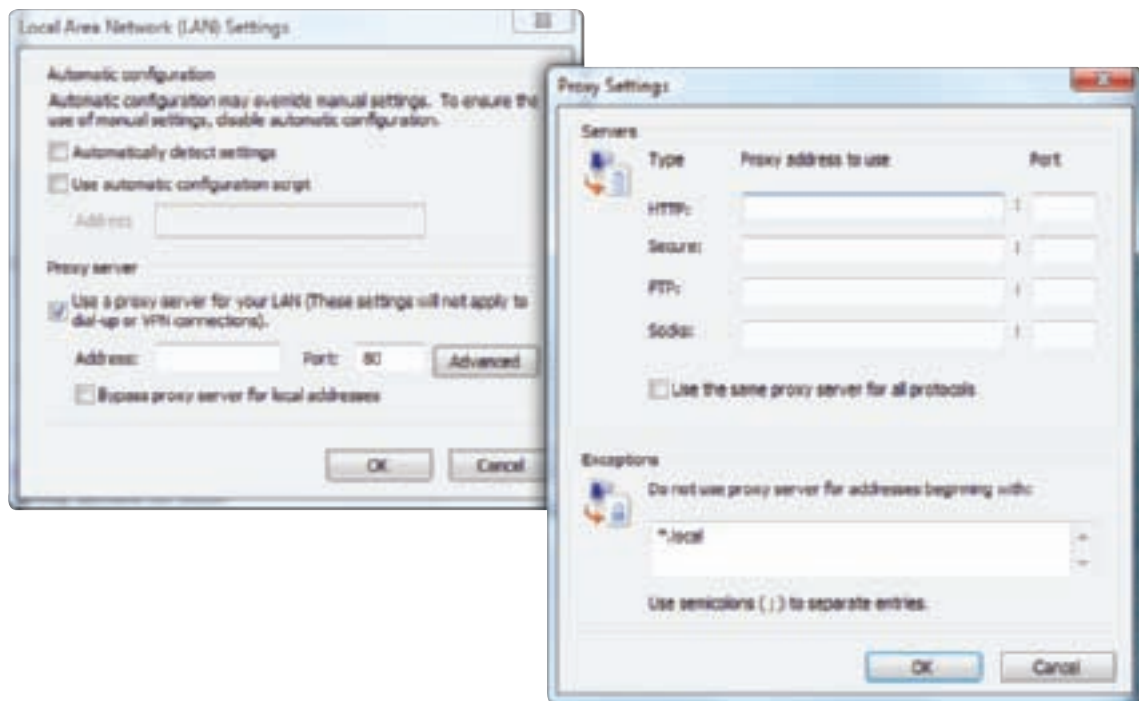
4. The access restriction feature of the router can also block certain Web sites (by URL) or block Web site content by keywords. Verify the content or site is not being blocked.
5. To verify that the router is not the problem with communication, you can connect a PC directly to the cable modem, DSL box, or other device so that the router is not involved. However, realize you're partially dropping your shields when you do so. First make sure that Windows Firewall and antivirus software is set for maximum protection, and don't leave the hardware firewall (router) out of the loop any longer than you need in order to solve the problem.

Sometimes security settings at your ISP might be a problem. For example, if you're trying to play an Internet game, you might need to contact your ISP and ask them to open a port that you need to play the game.

## PROXY SERVER CONNECTIONS

Many large corporations and ISPs use proxy servers to speed up Internet access. A **proxy server** is a computer that intercepts requests that a client makes of a server. It caches the Web pages and files that are requested. If another client requests the same content, the proxy server can provide the content that it has cached. When the proxy server needs to request content from a server, it substitutes its own IP address for the request in the same way that NAT works. In addition, proxy servers sometimes act as a gateway to the Internet, a firewall to protect the network, and to restrict Internet access by employees to force employees to follow company policies.

A Web browser does not have to be aware that a proxy server is in use; this type of proxy server, called a transparent proxy server, is the most common type. However, you can configure a Web browser to use a proxy server. To do that using Internet Explorer, click the **Connections** tab on the **Internet Options** box. Then click **LAN settings**. In the settings box, check **Use a proxy server for your LAN** and enter the IP address of the proxy server (see the left side of Figure 18-70). If your organization uses more than one proxy server, click **Advanced** and enter IP addresses for each type of proxy server on your network (see the right side of Figure 18-70). Click **OK** twice to close both boxes.



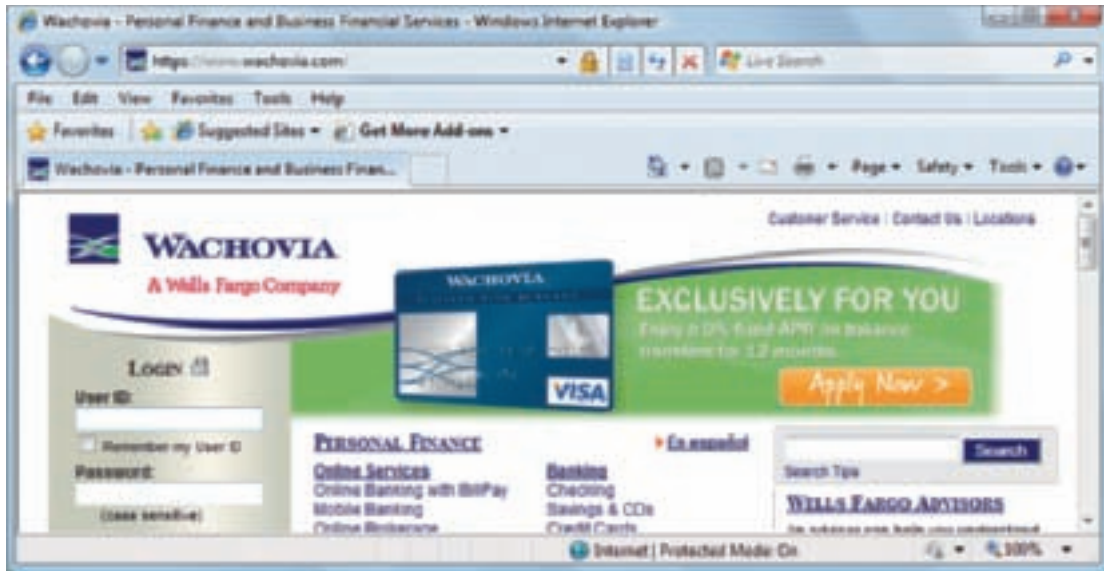
**Figure 18-70** Configure Internet Explorer to use one or more proxy servers  
Courtesy: Course Technology/Cengage Learning

## SECURED CONNECTIONS

Recall that two secure protocols that encrypt all transmissions are HTTPS and SSH. The purpose of these security protocols is to prevent others on the Internet from eavesdropping on data in transit or from changing that data. (This last type of intrusion is called a man-in-the-middle attack.)

To know if a connection to a Web site is secured using Internet Explorer version 7 or higher, look for https in the browser address box and a lock icon to the right of the address box (see Figure 18-71) or, in the case of earlier versions of IE, at the bottom of the window.

A+  
220-702  
3.1



**Figure 18-71** A secured connection from browser to Web server  
Courtesy: Course Technology/Cengage Learning

If you have a problem with connecting to a secured Web site from a corporate network, you might be using the wrong proxy server on the network. Check with your network administrator to find out if a specific proxy server should be used to manage secure Web site connections. If this is the case, click **Tools, Internet Options** to open the Internet Options box. Click the **Connections** tab and then click **LAN settings**. In the Local Area Network (LAN) Settings box, check **Use a proxy server for your LAN** and then click **Advanced** (refer back to Figure 18-70). In the box, notice that the second row can be used to enter the IP address of the proxy server that is to manage HTTPS connections.

Recall from Chapter 17 that an SSH client is sometimes used in place of Telnet to communicate with a remote computer when high security is needed. Using SSH (Secure Shell) client software, you can communicate with a remote computer and transfer files using a secure tunneling connection. Also, an SSH version of FTP (called Secure FTP or SFTP) can be used to make these types of connections secure. Windows does not contain an SSH client or server application, so third-party software must be used. Do the following if you are having a problem making an SSH connection:

- ▲ Verify that port forwarding is enabled on your router. SSH uses port 22.
- ▲ Using Windows Firewall, add port 22 to your exceptions list and allow exceptions.
- ▲ Using the IP address of the SSH server, ping the server to verify connectivity.
- ▲ Verify that you have the correct permissions on the remote SSH server.
- ▲ Check the Web site of the SSH software for other troubleshooting tips.

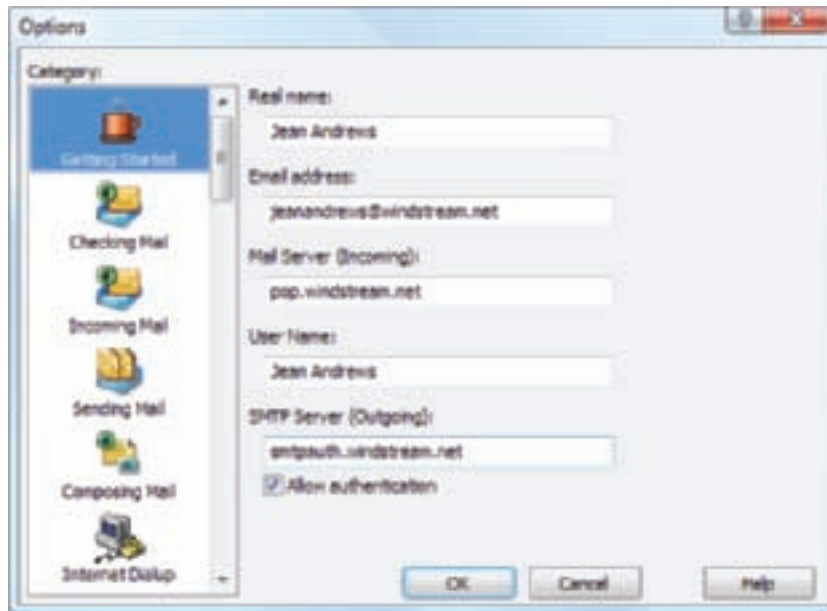
## E-MAIL CONNECTIONS

Problems with e-mail connections are likely caused by wrong client settings. Follow these steps to verify these critical settings:

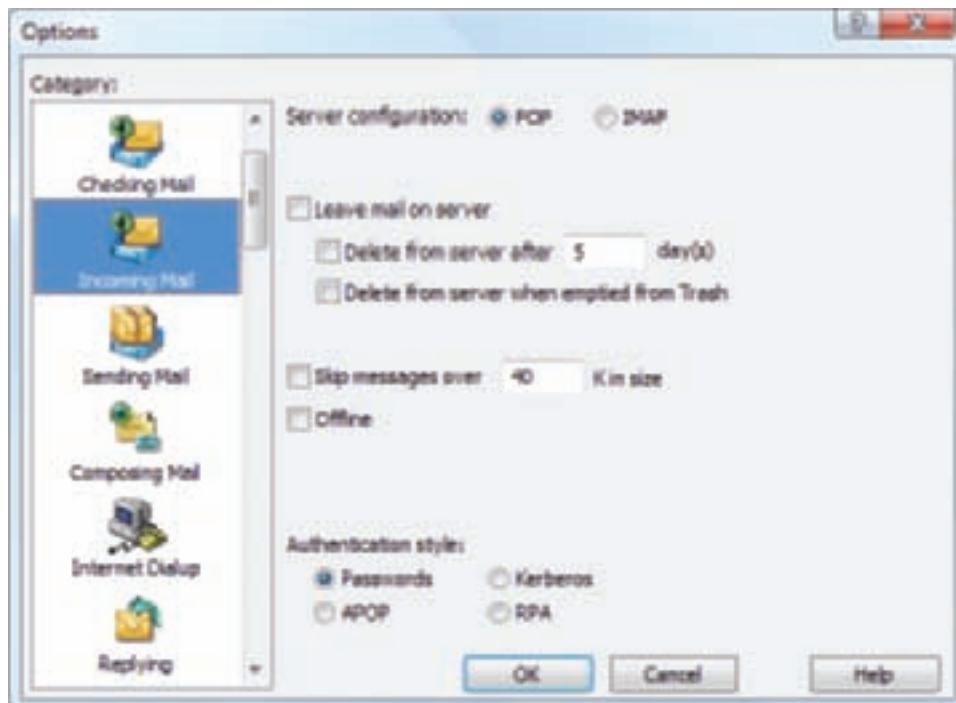
- ▲ Check the Web site of the ISP or other group that is managing the e-mail and find out the names of the outgoing and incoming e-mail servers and the protocols being used.



- ▲ In the e-mail client software, look for a way to view and change the incoming and outgoing mail servers. For example, in Figure 18-72, the incoming (receive e-mail) server is *pop.windstream.net* and the outgoing (send e-mail) server is *smtpauth.windstream.net*. The outgoing server is using the SMTP AUTH protocol.
- ▲ Verify the correct protocol is being used for incoming mail. Options are POP and IMAP (see Figure 18-73).



**Figure 18-72** Verify the correct e-mail servers are being used  
Courtesy: Course Technology/Cengage Learning



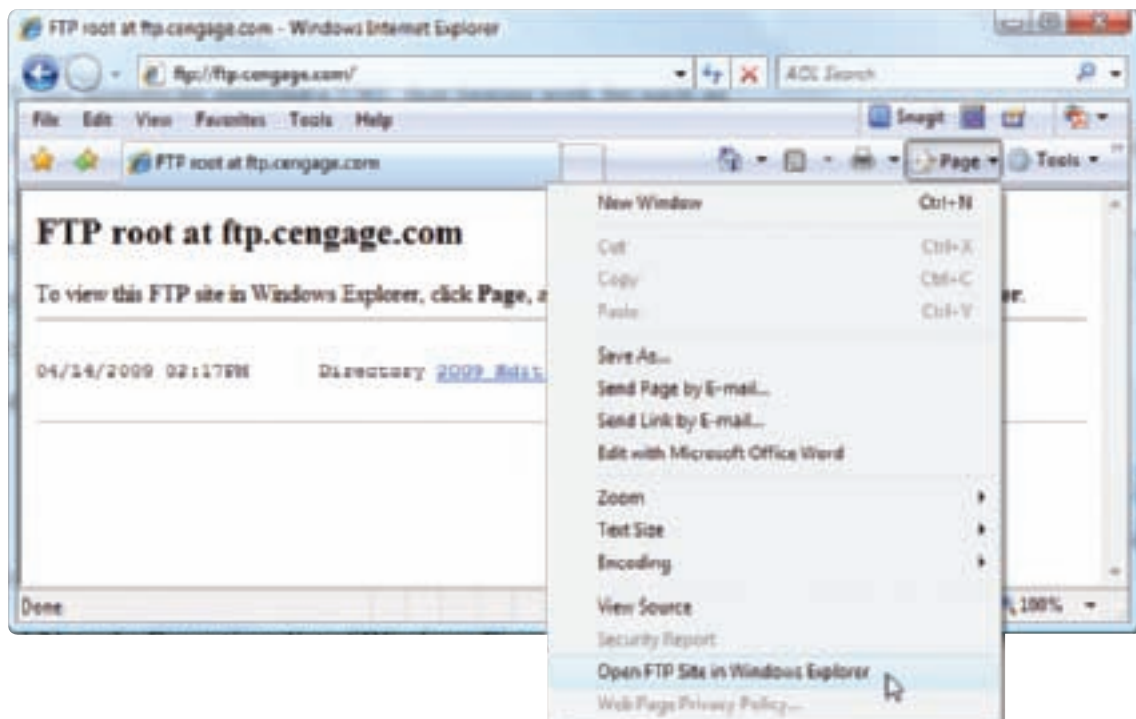
**Figure 18-73** Verify the incoming e-mail protocol  
Courtesy: Course Technology/Cengage Learning

A+  
220-702  
3.1

## FTP CONNECTIONS

The most popular way to transfer files over the Internet is to use the **File Transfer Protocol (FTP)**, which can transfer files between two computers using the same or different operating systems. Many software vendors use FTP sites for downloading software to their customers. When you click a link on a Web site to download a file, if the protocol in your browser address box changes from http to ftp, then you are using FTP for the download.

You can also access an FTP site directly by entering a URL that begins with ftp, such as ftp.cengage.com. If the site allows anonymous login, you will see a root level folder. If the site requires a login, a login box appears for you to enter a user account and password. Then the root level folder appears. To change the client application from Internet Explorer to Windows Explorer, on the **Page** menu, click **Open FTP Site in Windows Explorer** (see Figure 18-74). For Vista, a warning box appears asking permission to allow Internet Explorer to leave protected mode. Click **Allow**.



**Figure 18-74** Transferring files using FTP is best done with Windows Explorer  
Courtesy: Course Technology/Cengage Learning

If you are having problems using FTP, do the following:

- ▲ Add ports 20 and 21 to the Exceptions list of Windows Firewall.
- ▲ Ping the FTP server to make sure you have connectivity.
- ▲ Contact the administrator of the FTP site and verify that you have the correct permissions to the site.

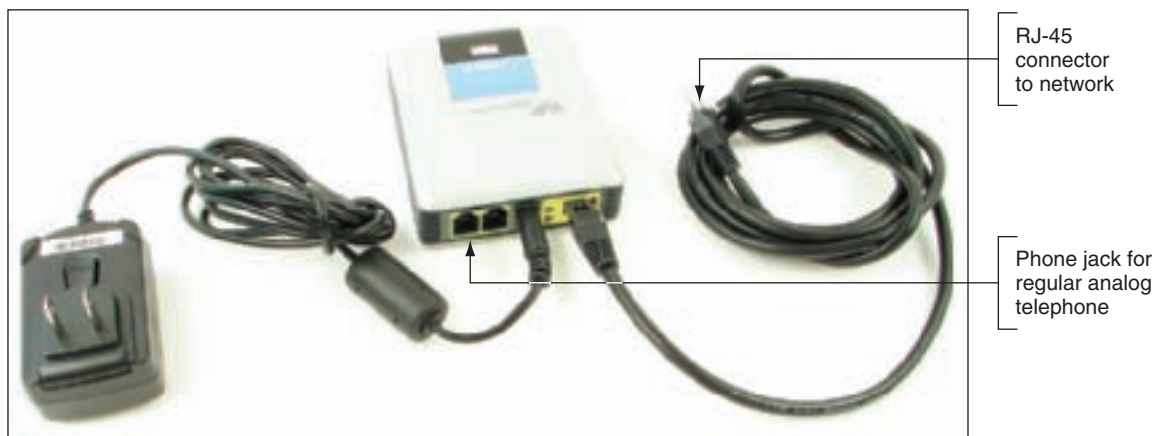
## VOIP CONNECTIONS

**VoIP (Voice over Internet Protocol)**, also called Internet telephone, provides voice communication over a network and uses the VoIP protocol. Using VoIP, voice is converted to digital data for transmission over the Internet and connects to the POTS (Plain Old Telephone Service) so that people without VoIP can make and receive calls from VoIP subscribers.

When setting up a VoIP service, you plug a digital telephone, such as the one shown in Figure 18-75, into a network port on a local network that is connected to the Internet and use that phone to make a phone call to anywhere on the planet. Notice in the figure, the power cord and network cable share a common cable and connector to the phone. You can also use a regular analog phone as an Internet phone if you use an Analog Telephone Adapter (ATA), such as the one shown in Figure 18-76. Plug the phone into the ATA, which uses a network cable to connect to the network. Just as with mobile phones, the digital phone or ATA is programmed for a particular phone number.



**Figure 18-75** This digital telephone has a network port to connect to a network  
Courtesy: Course Technology/Cengage Learning



**Figure 18-76** Use this ATA to turn an analog telephone into an Internet phone  
Courtesy: Course Technology/Cengage Learning

## APPLYING CONCEPTS

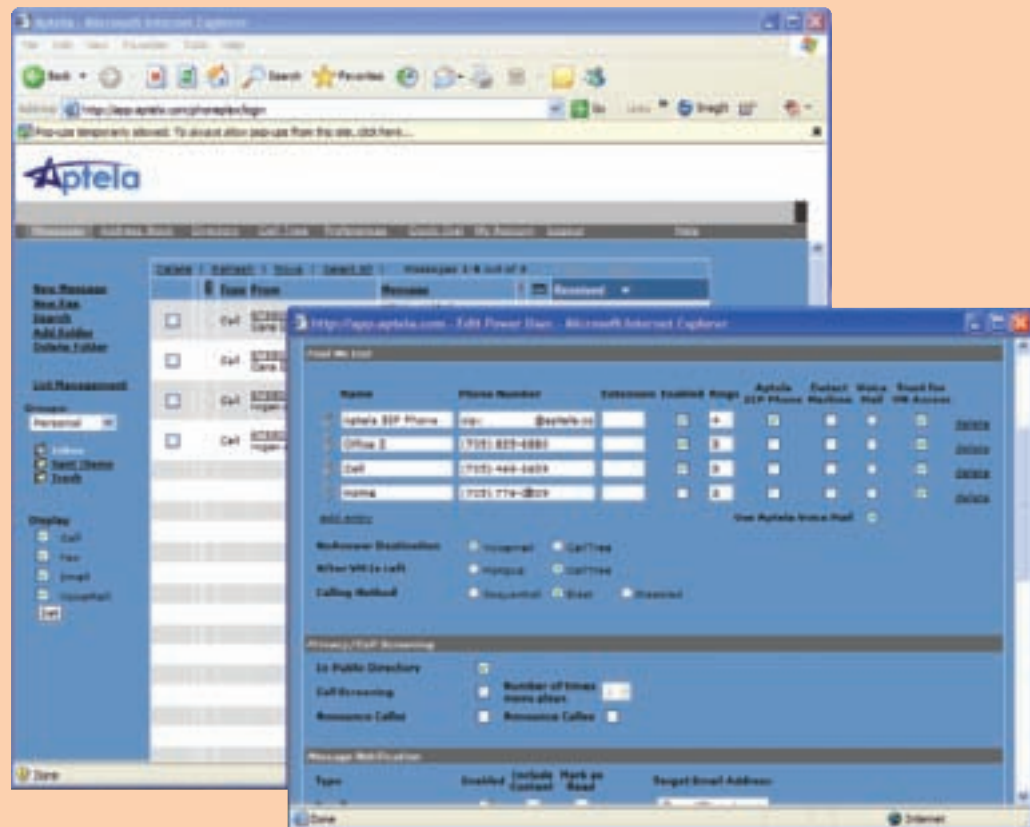
**Quality of Service (QoS)** refers to the success of communication over the Internet. Communication is degraded on the Internet when packets are dropped, delayed, delivered out of order, or corrupted. In order for VoIP to have the high quality it needs to compete with regular POTS voice communication, QoS on the Internet must be high. VoIP gave problems for many years with dropped lines, echos, delays, static, and jittered communication. ("Jitter" is the term used to describe a voice conversation that is mingled with varying degrees of delays.) However, more recently, many of these problems are for the most part solved to make VoIP a viable option for personal and business use. Recently, my

daughter, Jill West, was responsible for selecting a telephone system for a small business. I asked her to describe the successes and woes of having chosen a VoIP solution. Here is her story:

*We planned our company so that we all can work from our home offices and live in several regions of the country, yet we compete in a market where we must present a unified front. More and more businesses are built this way these days, and, thankfully, technology is adapting.*

*When we first began investigating phone systems, we tried to patchwork together various telco (local telephone company) services, but with dismal results. Then we began researching several VoIP providers, from the industry flagship Vonage (www.vonage.com), to smaller and lesser-known companies. With a little searching, we found a company that provides the services important to us. Here are a few features:*

- ▲ *We were able to buy the digital phones and ATA adapters from this company that configured and tested them for us before shipping and then taught us how to use them.*
- ▲ *We were able to port our existing toll-free number to our new VoIP account.*
- ▲ *We are able to transfer live calls from one team member to another with three- or four-digit dialing and no long-distance charges for the transferred calls, even with our team spread over several states.*
- ▲ *We have an integrated voice-mail system using a Web portal. One window of our portal is shown in Figure 18-77.*
- ▲ *We can easily set up conference calls with the entire team.*
- ▲ *A single auto-attendant handles all incoming calls, or we can direct incoming calls to any number and still use the auto-attendant as a convenient backup.*
- ▲ *The company provided professional voice talent to record our auto-attendant message and other call-tree menu options.*
- ▲ *We have unlimited long distance, even for our high-volume salespeople.*



**Figure 18-77** This Web portal is used to manage a VoIP service  
Courtesy: Course Technology/Cengage Learning

- ▲ We can add or remove users as our company's payroll changes with no extensive implementation charges or technical difficulties.
- ▲ Each of our users can program various phone numbers into their account, such as cell phone, home phone, or home-office phone numbers. They can then tell the system at which phone to direct their individual incoming calls. Each call can be sent sequentially through the list of numbers, or "blast" all numbers simultaneously.
- ▲ Voice-mail messages and faxes can all be forwarded to our various e-mail accounts, and even the message itself is attached for immediate review.
- ▲ When we travel, we can take the service with us. I can pack my IP phone or ATA and plug it up wherever I am if I have high-speed Internet access. Even without the phone or adapter, I can still use a computer to access my Web portal and make calls from the portal Web site.

*With all this, it seems there would be no drawbacks. But all is not well in paradise. We've had a few issues with dropped calls or annoying delays while talking. Sometimes we have to hang up and call the person back. Occasionally, the signal will phase out briefly, where one party can hear the other, but not vice versa. And, if your ISP drops your service for any reason, even just a temporary outage, you're pretty much without a phone. However, incoming calls are still directed through the auto-attendant, and messages are saved there until you again have access.*

*Overall, even with these drawbacks, VoIP was the right choice for our company. We're pleased with the features and are willing to tolerate the growing pains as technology catches up with our needs.*

When setting up a VoIP system, know that each digital phone or ATA must be programmed with a phone number from the VoIP provider. Each device is also programmed to use dynamic IP addressing and must be assigned an IP address just like any other device on the network, which means your network must be using a DHCP server, such as one provided by a multipurpose router. Plug up the devices to the network and then configure the VoIP service using the Web site of the VoIP provider.

Because electrical interference can be a problem with VoIP phones, each network cable connected to a VoIP phone needs a **ferrite clamp** (see Figure 18-78) attached. Attach the



**Figure 18-78** Install a ferrite clamp on a network cable to protect against electrical interference  
Courtesy: Course Technology/Cengage Learning



A+  
220-702  
3.1

clamp on the cable near the phone port. This clamp helps to eliminate electromagnetic interference (EMI). Some cables come with preinstalled clamps, and you can also buy ferrite clamps to attach to other cables.

## >> CHAPTER SUMMARY

- ▲ Cable modem and DSL boxes connect to a PC by way of a USB or network cable. They connect to a router using a network cable. The router provides additional firewall security to a network.
- ▲ If static IP addressing is used to connect to the Internet, you'll need to know the IP address assigned to you by your ISP, the IP address of one or two DNS servers, the subnet mask, and the IP address of the default gateway (the IP address of a server at the ISP). Static IP addressing is used for business accounts so that others on the Internet can initiate communication with services they provide.
- ▲ Satellite Internet access in North America uses a satellite dish that faces the southern sky.
- ▲ Vista can assign a public, private, or domain profile to a network connection. The assigned profile determines the degree of security applied. The profile with the highest security is a public profile.
- ▲ Vista manages network connections using the Network and Sharing Center, and XP manages connections using the Network Connections window.
- ▲ Windows Firewall is a software firewall that can provide varying degrees of security on a single computer.
- ▲ A wired network can use 10BaseT, 100BaseT, and 1000BaseT Ethernet. For fastest speeds, make sure all devices on the network use 1000BaseT.
- ▲ Local Ethernet networks use twisted pair (UTP or STP) cables rated at CAT5e or higher.
- ▲ Use a firewall on the host computer or router to protect the network from unsolicited activity from the network or Internet.
- ▲ It's extremely important to change the password to configure your router as soon as you install it, especially if the router is also a wireless access point.
- ▲ A router on a small network is most likely able to be configured to use DHCP, access restrictions, port filtering, port forwarding, and port triggering.
- ▲ Security for a wireless access point includes MAC address filtering, disabling SSID broadcasting, and encryption (WPA2, WPA, or WEP). The access point can also be a DHCP server.
- ▲ Use cable testers to test cables and trace network cables through a building.
- ▲ Useful Windows TCP/IP utilities are Getmac, Ipconfig, Net, Netstat, Nslookup, Ping, Telnet, and Tracert. Use third-party SSH client and server software to replace Telnet when a secured connection is needed.
- ▲ Remote Desktop and Remote Assistance can be used to connect remotely to a computer and manage the Windows desktop. Remote Desktop is better used to connect to your own computer, and Remote Assistance is designed to assist other users with their computers. Both use the RDP protocol.
- ▲ When troubleshooting network problems, check hardware, device drivers, Windows, and the client or server application, in that order.



**>> KEY TERMS**

For explanations of key terms, see the Glossary near the end of the book.

domain profile	port triggering	Remote Desktop
ferrite clamp	private profile	reverse lookup
File Transfer Protocol (FTP)	public profile	VoIP (Voice over Internet Protocol)
port filtering	Quality of Service (QoS)	
port forwarding	Remote Assistance	

**>> REVIEWING THE BASICS**

1. Give two popular examples of broadband technology.
2. Which type of broadband connection does Windows assume, on-demand or always-up?
3. What is the purpose of DSL filters on phone jacks in your home?
4. Which type of profile that Vista assigns to a network connection offers the least security?
5. What is the speed in bits per second of a 1000BaseT Ethernet network?
6. What is the maximum length of an Ethernet cable on a 100BaseT network?
7. What is the first configuration change you should make when you first install a router?
8. How is a DHCP reservation on a router used?
9. Which command is used to find the DNS server's information about a domain name?
10. Which command is used to find the host name of a computer when you know its IP address?
11. Which command can give you the hop count from your computer to another?
12. What parameter can be added to the Netstat command so that you can see what program is responsible for a network connection?
13. Which editions of Windows can be used to serve up Remote Desktop?
14. Which is the easiest way to initiate a Remote Assistance session?
15. What is the listening port for Windows XP Remote Desktop?
16. Which tool, Remote Desktop or Remote Assistance, allows you to set up a chat session with the user?
17. In what folder is a log of a Remote Assistance session kept?
18. How can you physically tell if a network card is not working?
19. To know if Windows recognizes a NIC without errors, which tool do you use?
20. What is the full command line to use Ipconfig to release the current IP address?
21. What is the full command line for the loopback address test?
22. What key do you press to refresh the Network window?
23. What command can tell you if two computers on the same network have the same computer name?
24. What command lists the shared resources on a remote computer on the network?

25. Which type of Net command can be used to map a network drive?
26. Which command tests for connectivity between two computers?
27. List the steps to recycle the connection to an ISP when using a cable modem and router.
28. If you want to allow an exception in Windows Firewall through a certain port, but the port or program is not listed under the Exceptions tab, what can you do?
29. When an ISP gives a user the two mail server addresses, smtp.myISP.net and pop.myISP.net, which address should be used for incoming mail and which should be used for outgoing mail?
30. What device is required so that you can connect a regular telephone to a VoIP network?

### >> THINKING CRITICALLY

1. You are trying to connect to the Internet using a Windows XP dial-up connection. You installed a modem card and tested it, so you know it works. Next, you create a dial-up connection icon in the Network Connections window. Then, you double-click the icon and the Connect dialog box opens. You click Dial to make the connection. An error message appears saying, "There was no dial tone." What is the first thing you do?
  - a. Check Device Manager for errors with the modem.
  - b. Check with the ISP to verify that you have the correct phone number, username, and password.
  - c. Check the phone line to see if it's connected.
  - d. Check the properties of the dial-up connection icon for errors.
2. You have set up a small LAN in your home with two Windows XP PCs connected to the Internet using a DSL connection. You have a DSL router box connected to the DSL and to a small switch. Your two PCs connect to the switch. You can browse the Internet from either PC. However, you discover that each PC cannot use the resources on the other PC. What is the problem and what do you do?
  - a. The network switch is not working. Try replacing the switch.
  - b. The NICs in each PC are not working. Try replacing one NIC and then the next.
  - c. The Local Area Connections in the Network Connections window are not working. Delete the connections and re-create them.
  - d. Files and folders are not shared on either PC. Use Windows Explorer to correct the problem.
3. You connect to the Internet using a cable modem. When you open your browser and try to access a Web site, you get the error: "The Web page you requested is not available offline. To view this page, click Connect." Select two explanations and their solutions that are reasonable and might work. Select two explanations and solutions that are not reasonable and explain why they won't work.
  - a. The browser has been set to work offline. On the File menu, verify that Work Offline is not checked.
  - b. The connection to the cable modem is down. In the Network and Sharing Center, click view status for the LAN connection and select Diagnose.

- c. Windows Firewall is enabled on your PC. Disable it.
- d. The cable modem is not working. Go to Device Manager and check for errors with the cable modem.

## >> HANDS-ON PROJECTS

### PROJECT 18-1: Practicing TCP/IP Networking Skills

While connected to the Internet or another TCP/IP network, answer these questions:

1. What is your current IP address?
2. Release and renew your IP address. Now what is your IP address?
3. Are you using dynamic or static IP addressing? How do you know?
4. What is your adapter address for this connection?
5. What is your default gateway IP address?
6. What response do you get when you ping the default gateway?

### PROJECT 18-2: Researching Remote Assistance

A technician needs to know how to find information he needs to help users and troubleshoot problems. Using sources you can trust, answer the following. List your source of information for each question.

1. What are the steps to cancel a Remote Assistance invitation before it expires?
2. What are the steps to extend a Remote Assistance invitation from six to 12 hours?
3. What are the steps to start a Remote Assistance session when using Windows Messenger?
4. What is the time until expiration for an invitation when using Windows Vista? When using Windows XP?

### PROJECT 18-3: Investigating Verizon FiOS

Verizon ([www.verizon.com](http://www.verizon.com)) is currently offering an alternative to DSL and cable modem for broadband Internet access. FiOS is a fiber-optic Internet service that uses fiber-optic cable all the way to your house for both your residential telephone service and Internet access. Search the Web for answers to these questions about FiOS:

1. Give a brief description of FiOS and how it is used for Internet access.
2. What downstream and upstream speeds can FiOS support?
3. When using FiOS, does your telephone voice communication share the fiber-optic cable with Internet data?
4. What does Verizon say about FiOS cabling used for television?
5. Is FiOS available in your area?

**PROJECT 18-4:** Practicing Using FTP

Practice using FTP by downloading the latest version of Firefox, a Web browser, using three different methods. Do the following:

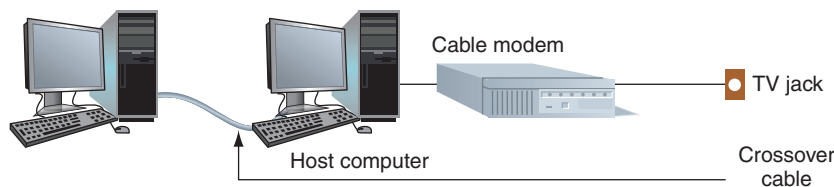
1. Using your current browser, go to the Mozilla Web site at *www.mozilla.org* and download the latest version of Firefox. What is the version number? What is the name of the downloaded file? In what folder on your hard drive did you put the file?
2. Using your current browser as an FTP client, locate the same version of Firefox and the same file at the Mozilla FTP site (*ftp.mozilla.org*) and download it to your PC. What is the path to the Firefox file on the FTP site? In what folder on your hard drive did you put the file?

**PROJECT 18-5:** Teaching Yourself About Windows Meeting Space

Using the Windows Help and Support window, search for information on Windows Meeting Space. Describe the tool. When would you want to use it? What can you do with Windows Meeting Space? Set up and test the tool with a friend on a network connection.

**>> REAL PROBLEMS, REAL SOLUTIONS****REAL PROBLEM 18-1:** Firewalling Your Home Network

At first, Santiago had only a single desktop computer, an ink-jet printer, and a dial-up phone line to connect to the Internet. Then, his wife, Maria, decided she wanted her own computer. Later they both decided it was time for a broadband connection to the Internet and chose cable. So now, their home network looks like that shown in Figure 18-79. Santiago chose to use a crossover cable to connect the two computers, and the cable modem connects to Santiago's computer using a USB cable. The computer connected to the Internet uses Internet Connection Sharing to serve up Internet access to the other computer.



**Figure 18-79** Two networked computers sharing an Internet connection  
Courtesy: Course Technology/Cengage Learning

Both computers are constantly plagued with pop-up ads and worms, so Santiago has come to you for some advice. He's heard he needs to use a firewall, but he doesn't know what a firewall is or how to buy one. You immediately show him how to turn on Windows Firewall on both Vista PCs, but you know he really needs a better hardware solution. What equipment (including cables) do you recommend he buy to implement a hardware firewall? Also consider that his daughter, Sophia, has been begging for a notebook computer for her birthday, so plan for this expansion. By the way, Sophia has made it perfectly clear there's no way she'll settle for having to sit down in the same room with her parents to surf the Web, so you need to plan for a wireless connection to Sophia's bedroom.

**REAL PROBLEM 18-2:** More Security for Remote Desktop

When Jacob travels on company business, he finds it's a great help to be able to access his office computer from anywhere on the road using Remote Desktop. However, he wants to make sure his office computer as well as the entire corporate network is as safe as possible. One way you can help Jacob add more security is to change the port that Remote Desktop uses. Knowledgeable hackers know that Remote Desktop uses port 3389, but if you change this port to a secret port, hackers are less likely to find the open port. Search the Microsoft Knowledge Base articles ([support.microsoft.com](http://support.microsoft.com)) for a way to change the port that Remote Desktop uses. Practice implementing this change by doing the following:

1. Set up Remote Desktop on a computer to be the host computer. Use another computer (the client computer) to create a Remote Desktop session to the host computer. Verify the session works by transferring files in both directions.
2. Next, change the port that Remote Desktop uses on the host computer to a secret port. Print a screen shot showing how you made the change. Use the client computer to create a Remote Desktop session to the host computer using the secret port. Print a screen shot showing how you made the connection using the secret port. Verify the session works by transferring files in both directions.
3. What secret port did you use? What two Microsoft Knowledge Base Articles gave you the information you needed?

*This page intentionally left blank*